



UFED Logical Analyzer

Manuel de l'utilisateur

Décembre 2014

Avis juridiques

Ce manuel fourni est sujet aux conditions et restrictions suivantes :

- Ce manuel contient des informations propriétaires appartenant à Cellebrite Mobile Synchronization Ltd. De telles informations sont fournies uniquement dans le but d'assigner explicitement et correctement les utilisateurs autorisés au UFED Logical Analyzer.
- Aucune partie de ce contenu ne peut être utilisée à d'autres fins, dévoilée à toute personne ou société, ou reproduite de toute manière, électronique ou mécanique, sans l'autorisation expresse préalable et écrite de Cellebrite Ltd.
- Les textes et graphiques sont donnés dans un but d'illustration et de référence seulement. Les spécifications sur lesquelles ils sont basés sont sujettes à modification sans préavis.
- Les informations contenues dans ce document sont sujettes à modification sans préavis. Les noms et données d'entreprise et de personnes utilisés ici dans des exemples sont fictifs sauf mention contraire.

Contenu


cellebrite
delivering mobile expertise

Chapitre 1 : **Introduction**

Bienvenue dans UFED Logical Analyzer. UFED Logical Analyzer est une application qui lit les fichiers UFED (fichiers de vidage UFED *.ufd) et les fichiers de rapport UFED (*.xml) créés dans le cadre de l'extraction numérique, et le package de rapport UFED (*.ufdr) généré à partir des données analysées d'une extraction numérique par UFED Logical Analyzer.

UFED Logical est divisé en deux composants :

- L'appareil UFED avec modules Logical, utilisé pour créer une extraction numérique d'appareils mobiles ou de cartes SIM, qui peut ensuite être enregistrée sur une clé USB, une carte mémoire SD ou directement sur votre PC.
- L'application UFED Logical Analyzer, qui permet aux investigateurs d'effectuer une analyse en profondeur des données extraites dans le cadre d'une extraction numérique.

UFED Logical fonctionne en deux étapes :

- Extraction numérique avec l'appareil UFED,
- Analyse et la génération de rapports à l'aide de UFED Logical Analyzer.



UFED Logical Analyzer vous permet d'ouvrir des rapports UFED, d'effectuer vos propres recherches et analyses sur les informations analysées, et d'effectuer des actions telles que la recherche, la création de rapports, la création de signets d'entités, etc.

Chapitre 2 : **Installation et activation**

Ce chapitre décrit le processus d'installation et d'activation de UFED Logical Analyzer sur votre PC.



2.1. Installer UFED Logical Analyzer

2.1.1. Configuration requise

PC	PC compatible avec Windows, avec processeur Pentium® IV ou compatible, fonctionnant à 1,6 GHz ou plus
Système d'exploitation	Microsoft Windows XP[1] avec SP3 ou plus récent Microsoft Windows Vista™, Windows 7 ou Windows 8
Mémoire (RAM)	Système d'exploitation / Recommandé / Minimum 32 bits / 4 Go / 4 Go 64 bits / 8 Go / 4 Go
Espace requis	500 Mo d'espace libre sur le disque pour l'installation
Conditions supplémentaires	Microsoft® .Net version 4.0 REMARQUE : Windows XP 64 bits nécessite l'installation d'un correctif .Net 2.0 (NDP20-KB913384-X64.exe), téléchargeable à l'adresse http://archive.msdn.microsoft.com/KB913384/Release/ProjectReleases.aspx?ReleaseId=771

[1] À compter du 28 février 2015, la série UFED ne prendra plus en charge Windows XP.

Autorisations	Si vous avez l'intention d'activer l'application à l'aide d'une clé de licence logicielle (dongle) fournie par Cellebrite, vous devez disposer de droits d'administrateurs sur l'ordinateur.

REMARQUE : Pour permettre l'extraction vers un PC avec le système d'exploitation Windows Vista, suivez la procédure décrite dans la section ***Permettre la connectivité avec Windows Vista*** (page ***30***).

2.1.2. Installation du logiciel

2.1.2.1. Obtenir une copie de UFED Logical Analyzer

Vous pouvez trouver une copie du logiciel d'installation le plus récent pour l'application UFED Logical Analyzer auprès des sources suivantes :

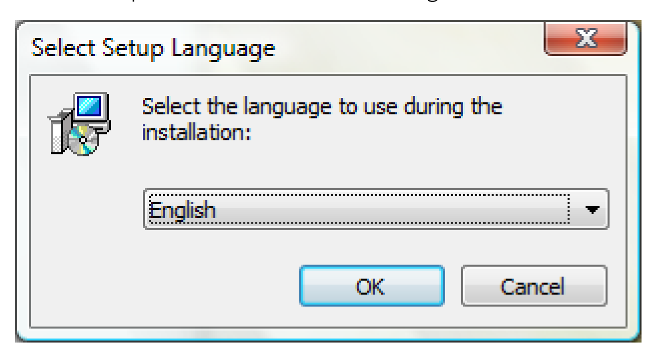
- En le téléchargeant sur le site MyCellebrite.
- En le téléchargeant à l'aide du lien fourni dans les notes de publication.



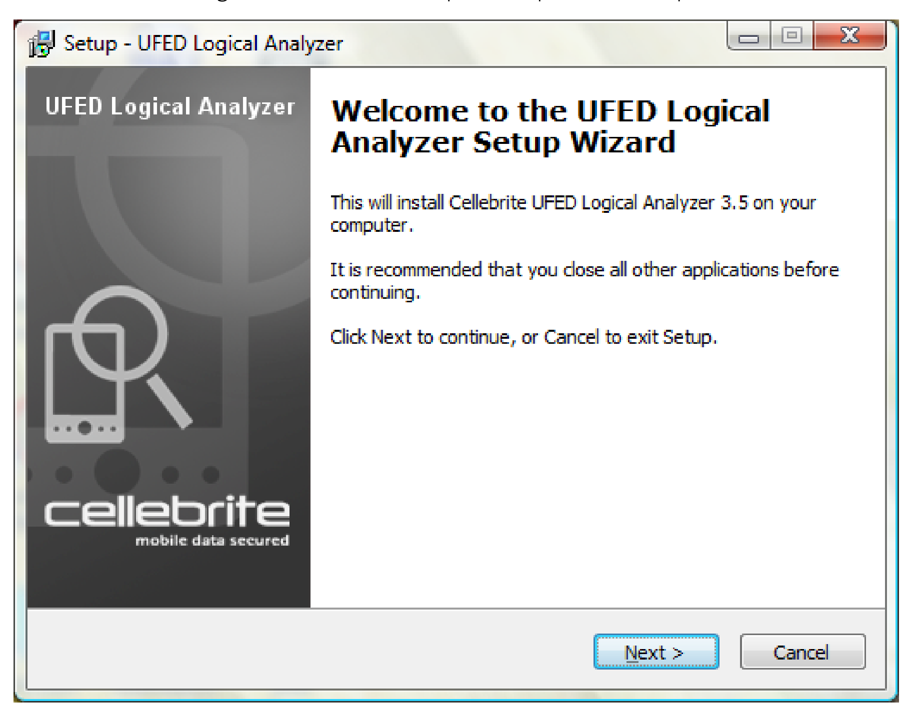
2.1.2.2. Installer UFED Logical Analyzer

REMARQUE : Avant de commencer, assurez-vous qu'aucun câble U-441 n'est branché à votre ordinateur.

1) Double-cliquez sur le fichier de configuration.

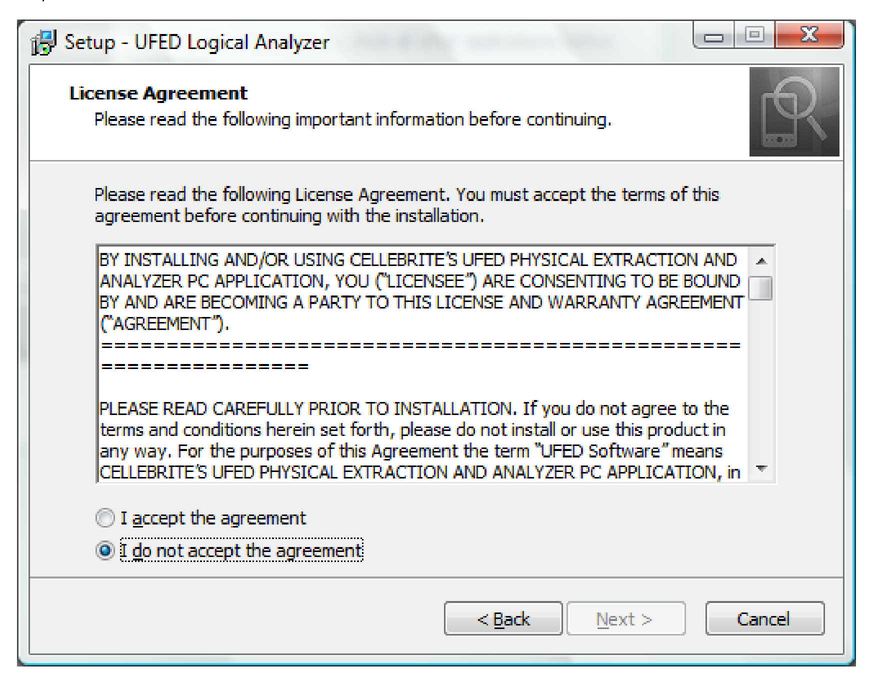


2) Sélectionnez la langue de votre choix, puis cliquez sur **OK** pour continuer.

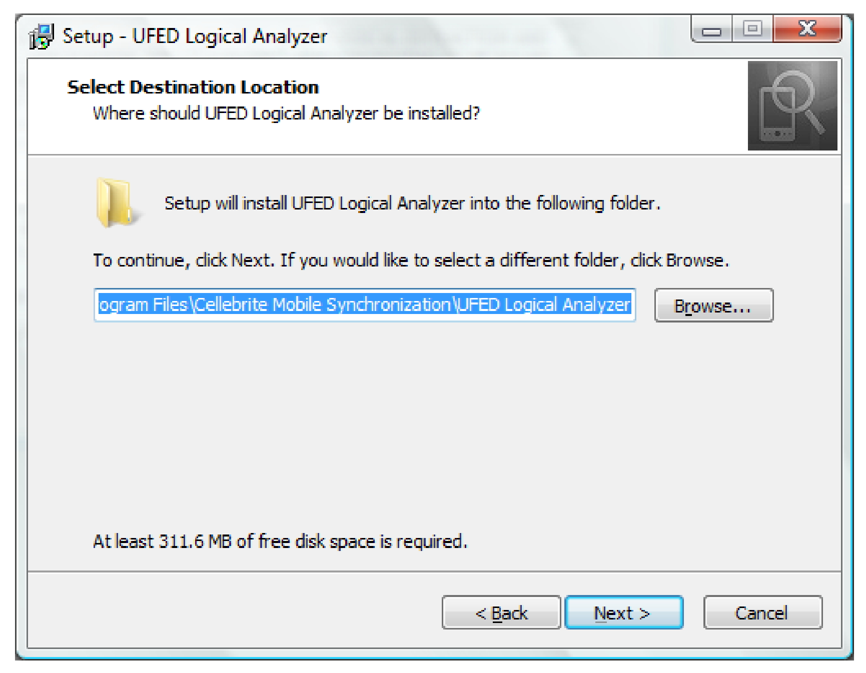




3) Cliquez sur **Suivant**.



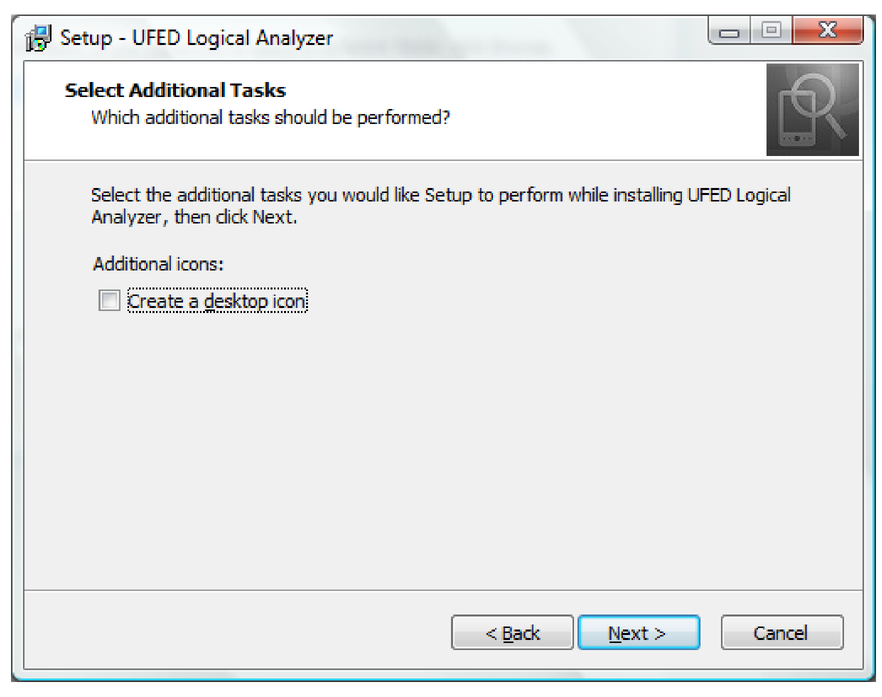
4) Sélectionnez **J'accepte l'accord**, puis cliquez sur **Suivant**.



5) Si vous le souhaitez, cliquez sur **Parcourir** pour choisir un dossier d'installation différent.

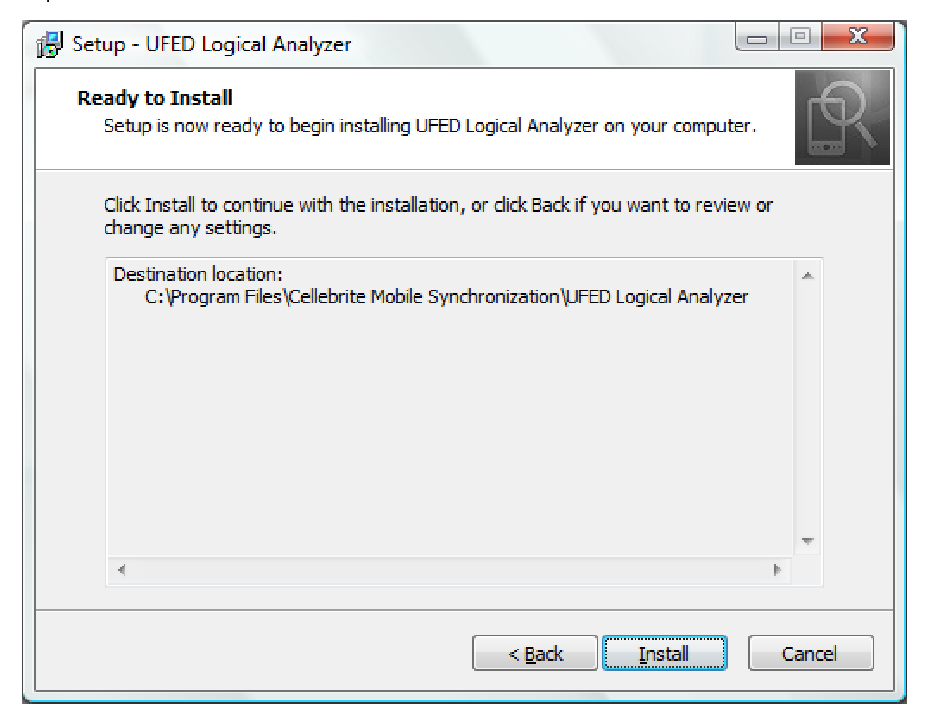


6) Cliquez sur **Suivant**.



7) Si vous ne souhaitez pas qu'une icône soit placée sur le bureau, décochez la case **Créer une icône sur le bureau**.

8) Cliquez sur **Suivant**.



9) Cliquez sur **Installer**. L'installation commence.



REMARQUE : Dans le cadre du processus d'installation, il peut vous être demandé de télécharger et d'installer Microsoft .NET 3.5 Framework. Un accès à Internet depuis votre ordinateur est nécessaire pour effectuer cette installation.

Setup - UFED Logical Analyzer

UFED Logical Analyzer

cellebrite
mobile data secured

Completing the UFED Logical Analyzer Setup Wizard

Setup has finished installing UFED Logical Analyzer on your computer. The application may be launched by selecting the installed icons.

Click Finish to exit Setup.

- [ ] Install HASP Dongle drivers (you can uncheck this item if you have already installed these drivers before)
- [x] Launch UFED Logical Analyzer

Finish

10) Si vous avez l'intention d'activer l'application à l'aide d'une clé de licence logicielle (dongle) fournie par Cellebrite, vous devez sélectionner **Installer les pilotes de dongle HASP**.

    REMARQUE : Vous devez disposer de droits d'administrateur pour installer les pilotes de dongle HASP.

11) Pour lancer UFED Logical Analyzer à la fin de l'installation, sélectionnez **Lancer UFED Logical Analyzer**.
12) Cliquez sur **Terminer**.

2.1.3. Activer UFED Logical Analyzer

Pour activer UFED Logical Analyzer, utilisez l'une des méthodes suivantes :

- Utilisez une clé de licence (dongle)
- Utiliser une licence logicielle
- Utiliser une clé réseau (dongle)

2.1.3.1. Notification de nouvelle version

Cellebrite vous informe lorsqu'une nouvelle version de votre logiciel est disponible. Si vous êtes connecté à Internet, vous recevrez cette notification lorsque la nouvelle version est disponible. Si vous n'êtes pas connecté à Internet, cette notification s'affiche tous les 3 mois.



2.1.3.2. Utiliser une clé de licence (dongle)



Clé de licence
(dongle) UFED

Utilisez le dongle UFED fourni dans votre kit UFED. Le dongle contient les licences de toutes les applications achetées.

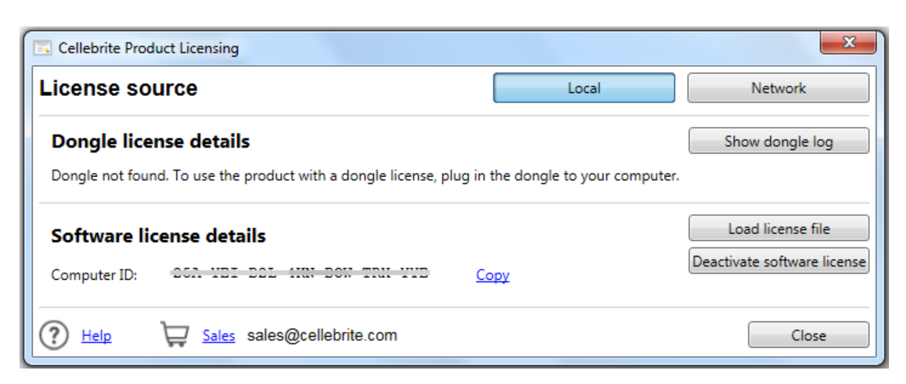
Pour utiliser UFED Logical Analyzer avec un dongle :

1) Connectez le dongle à un port USB de votre ordinateur. La licence est automatiquement détectée. Une fois le dongle reconnu par le système d'exploitation, l'application peut lire la licence.
2) Lancez UFED Logical Analyzer.

   Félicitations ! Votre application est maintenant prête à l'emploi.

Si la clé de licence (dongle) est introuvable :

1) Lorsque vous le lancez pour la première fois, ou lorsqu'une clé de licence est introuvable, la fenêtre « Licence du produit Cellebrite » s'affiche.



2) Si vous avez connecté le dongle à un port USB sur votre ordinateur, et qu'il ne fonctionne toujours pas, contactez-nous à l'adresse support@cellebrite.com.

REMARQUE : Les pilotes du dongle HASP doivent être installés pour pouvoir utiliser une clé de licence matérielle. Si les pilotes n'ont pas été installés lors du processus d'installation du logiciel UFED, vous pouvez exécuter le processus d'installation à nouveau, et sélectionner Installer les pilotes du dongle Hasp à la fin du processus.

2.1.3.3. Utilisation de l'application avec une clé logicielle

Vous devez activer la licence lors du premier démarrage de l'application.

Pour utiliser UFED Logical Analyzer avec une licence logicielle :

1) Cliquez sur le lien suivant : https://my.cellebrite.com/logicalanalyzer



2) Connectez-vous à votre compte MyCellebrite.

   (Si vous ne possédez pas de compte, cliquez sur **Inscrivez-vous maintenant**, créez un utilisateur, puis retournez au lien vers l'application UFED souhaitée.)

   Vous êtes alors dirigé sur la fenêtre d'activation du produit.

3) Cliquez sur Télécharger l'application et enregistrez le fichier sur le PC.
4) Extrayez le fichier Zip, cliquez sur le fichier d'installation et installez le logiciel à l'aide de l'assistant d'installation. Redémarrez l'ordinateur si cela vous est demandé.
5) Répétez l'étape 1 pour accéder au lien vers l'application.
6) Dans la fenêtre Méthode d'activation, si vous avez acheté UFED 4PC, sélectionnez **Code d'activation** ou si vous avez acheté UFED Touch, sélectionnez **UFED Touch/UFED Classic**.

   Activation Method | Activation Code

   Activation Method | UFED Touch/UFED Classic

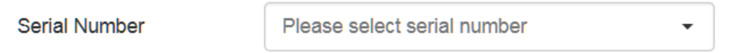
7) Selon le produit que vous avez acheté, continuez de la façon suivante :
   - **UFED 4PC :** Dans le champ Code d'activation, entrez le code d'activation fourni avec le kit UFED 4PC.

     Activation Code

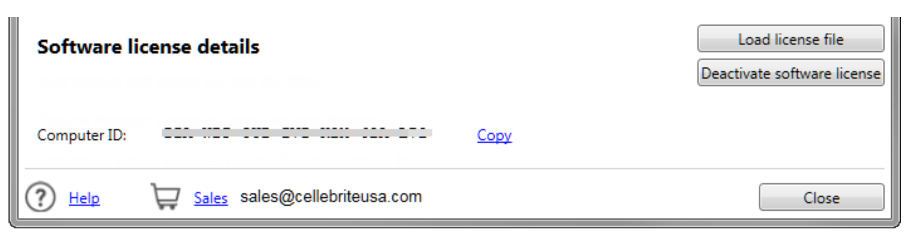


Code

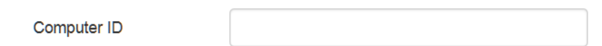
- **UFED Touch :** Dans le champ Choisir le numéro de série, sélectionnez le numéro de série UFED affiché sur l'unité UFED Touch ou sur l'écran Activation de la licence UFED Touch.



8) Récupérez ensuite l'ID ordinateur (ne fermez pas la page MyCellebrite lors de cette étape).
   - Lancez l'application. La fenêtre « Licence de produit Cellebrite » s'affiche.
   - Cliquez sur **Copier** pour copier l'ID ordinateur affiché à l'écran.



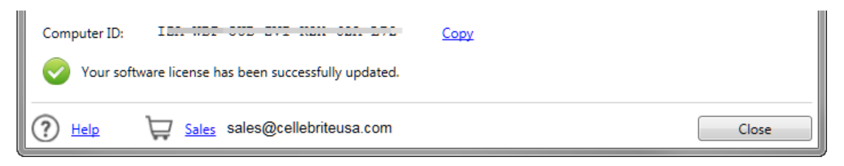
9) Sur MyCellebrite, collez l'ID ordinateur copié.



10) Cliquez sur **Télécharger maintenant !** pour télécharger la clé de licence de votre application sur votre PC. La clé de licence est également envoyée à votre adresse e-mail enregistrée sur MyCellebrite.
11) Dans l'application, cliquez sur **Charger le fichier de licence** dans la fenêtre Licence de produit Cellebrite.



12) Sélectionnez le fichier « License » et cliquez sur **Ouvrir**. Un message s'affiche pour vous indiquer que la licence logicielle a bien été mise à jour.



13) Cliquez sur **Fermer**.

Félicitations ! Votre application est maintenant prête à l'emploi.

2.1.3.4. Utiliser une clé réseau (dongle)

La clé réseau est connectée au réseau de votre entreprise et contient les licences de toutes les applications achetées.

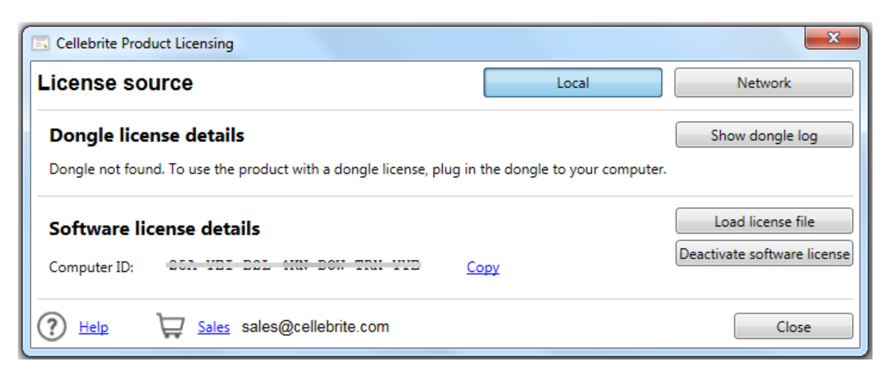


Clés réseau UFED

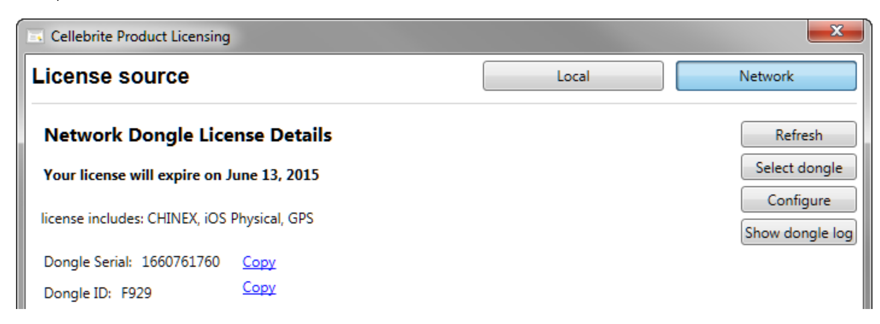
Pour utiliser UFED Logical Analyzer avec une clé réseau :

14) Lancez l'application UFED. Si la clé réseau est connectée au réseau, l'application démarre et l'utilisateur peut commencer à travailler immédiatement.

Si la clé réseau n'est pas reconnue, la fenêtre « Licence de produit Cellebrite » s'affiche.



15) Cliquez sur **Réseau**. La fenêtre suivante s'affiche :





REMARQUE : Si aucune clé n'est trouvée sur le réseau, assurez-vous d'être connecté à Internet et qu'une clé est connectée au réseau. Cliquez ensuite sur **Rafraîchir** pour rechercher une clé réseau à nouveau.

REMARQUE : Par défaut, la configuration du réseau est Diffusion. Si nécessaire, vous pouvez connecter manuellement la clé réseau. Cliquez sur **Configurer** pour modifier la configuration du réseau et choisissez l'option Hôte spécifique. Saisissez le nom de l'hôte (ou son adresse IP) et le numéro de port (1 à 5 chiffres).

REMARQUE : Si une seule clé réseau est disponible, elle est sélectionnée automatiquement. S'il y a plusieurs clés réseau, sélectionnez la clé souhaitée dans la liste, puis cliquez sur **Appliquer**.

Félicitations ! Votre application est maintenant prête à l'emploi.

2.1.4. Déplacer UFED Logical Analyzer vers un autre PC à l'aide d'une licence logicielle

Lorsqu'une installation de UFED Logical Analyzer activée par une licence logicielle doit être déplacée vers un autre PC, vous devez d'abord désactiver (supprimer) la licence de l'ordinateur d'origine.

1) Dans UFED Logical Analyzer, allez dans **Aide** > **Afficher les détails de la licence**.

   La fenêtre « Licence de produit Cellebrite » s'affiche.

2) Cliquez sur **Désactiver la licence logicielle**.

   La fenêtre « Désactivation de la licence logicielle » s'affiche.

3) Cliquez sur **Copier** pour copier l'identifiant de l'ordinateur.
4) Rendez-vous sur la page **http://my.cellebrite.com/deactivation**, et connectez-vous à votre compte MyCellebrite.

   Si vous n'avez pas de compte, cliquez sur **Inscription** et créez un utilisateur. Puis revenez à la page **http://my.cellebrite.com/deactivation**.

   Vous êtes alors dirigé vers l'assistant de désactivation.

5) Collez l'identifiant de l'ordinateur, puis cliquez sur **Suivant**.
6) Cliquez sur **Télécharger** et téléchargez le fichier de désactivation sur votre ordinateur.
7) Dans UFED Logical Analyzer, allez dans **Aide** > **Afficher les détails de la licence**.
8) Cliquez sur **Sélectionner le fichier de désactivation**, puis sélectionnez le fichier de désactivation téléchargé à l'étape 6.

   Votre licence est désactivée, et UFED Logical Analyzer crée un fichier de désactivation. La fenêtre « Désactivation de la licence logicielle » vous informe que le fichier de désactivation a été créé.

9) Revenez à l'assistant de désactivation dans **http://my.cellebrite.com/deactivation**.
10) Cliquez sur **Choisir le fichier**, puis téléchargez le fichier de désactivation créé par UFED Logical Analyzer.



11) Cliquez sur **Terminer**.
12) Pour obtenir votre nouvelle licence UFED Logical Analyzer, rendez-vous à l'adresse **http://my.cellebrite.com/logicalanalyzer**, et suivez les étapes d'activation de la licence. Pour plus d'informations, consultez la section ***Activer UFED Logical Analyzer*** (page *21*).

2.1.5. Permettre la connectivité avec Windows Vista

Suivez la procédure ci-dessous pour permettre à l'unité UFED de se connecter aux ordinateurs sur lesquels le système d'exploitation Windows Vista est installé.

1) Accédez au dossier Cellebrite Physical Analyzer **Drivers\cbrtucbl**.
2) Double-cliquez sur **USB_Cable_DRV.exe**.
3) Suivez les instructions à l'écran.

Chapitre 3 : **Mise en route**

UFED Logical Analyzer propose des outils de présentation et d'analyse puissants pour les données extraites d'un appareil, et simplifie la tâche de navigation au sein des types de données de l'appareil. UFED Logical Analyzer vous assiste dans l'exécution de tâches complexes telles que la collecte d'informations, la recherche d'investigation et la création de rapports constituant des preuves légales.

Cette application est conçue pour utiliser l'extraction numérique de l'unité UFED sous forme claire et concise, permettant aux investigateurs d'utiliser des outils de recherche puissants pour analyser et décoder les informations pertinentes.

Enfin, une dernière étape vous permet de créer des rapports avec vos trouvailles et de les exporter dans plusieurs formats de fichier, tels que UFDR, HTML, PDF, Excel (*.xlsx) et XML.

3.1. Lancer UFED Logical Analyzer

Pour lancer UFED Logical Analyzer, utilisez l'une des méthodes suivantes :

- Double-cliquez sur le raccourci bureau de **UFED Logical Analyzer**.
- Sélectionnez **Démarrer > Programmes > Cellebrite Mobile Synchronization > UFED Logical Analyzer**.



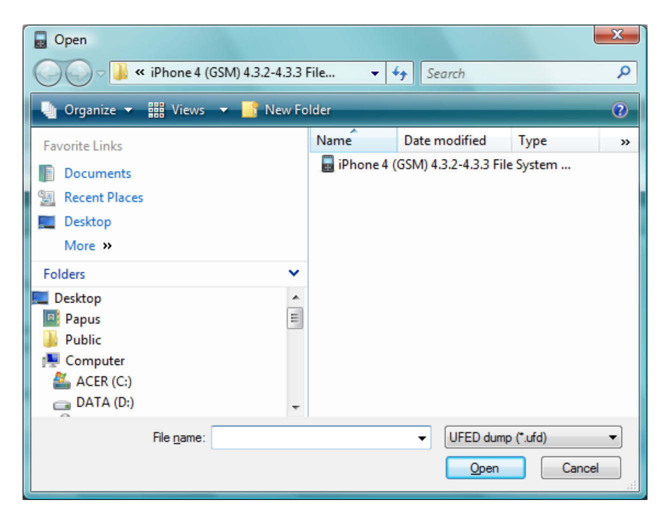
Pour une présentation de l'espace de travail, consultez la section ***S'orienter dans l'espace de travail*** (page ***45***).

3.2. Ouvrir un fichier pour analyse

UFED Logical Analyzer permet d'ouvrir les fichiers UFD créés par l'appareil UFED avec des modules numériques, les fichiers XML créés par UFED Physical Analyzer et les fichiers UFDR.

1) Utilisez une des méthodes suivantes :

- Dans l'onglet **Accueil**, cliquez sur **Ouvrir**.
- Glissez-déposez le fichier UFD dans UFED Logical Analyzer.
- Dans la barre d'outils de l'application, cliquez sur .
- Dans le menu de l'application, sélectionnez **Fichier** > **Ouvrir**.



2) Utilisez une des méthodes suivantes :

- Accédez à l'emplacement du fichier, sélectionnez-le et cliquez sur **Ouvrir**.
- Faites un glisser-déposer du fichier sur UFED Logical Analyzer.

Le processus d'analyse des données commence. Cela peut durer plusieurs secondes. À la fin du processus, un nouveau projet est ajouté à l'**arborescence de projet** et le **Résumé d'extraction** apparaît dans la zone d'affichage des données.



3.3. Extraction de données vers un PC

1) Utilisez une des méthodes suivantes :

- Connectez votre appareil UFED à votre PC à l'aide d'un câble USB ou mini-USB, en utilisant le port marqué « PC » sur le dessus de votre unité UFED. Vous pouvez être invité à installer des pilotes sur votre PC (voir le Manuel de l'utilisateur UFED Touch).
- Connectez votre appareil UFED à votre PC à l'aide du câble PC (U-441) fourni dans les kits UFED standard et tout-terrain. Vous pouvez être invité à installer des pilotes sur votre PC (voir le Manuel de l'utilisateur UFED Touch).



Image 1 : Câble UFED à PC

2) Connectez l'appareil source, à l'aide d'un câble adapté, au port USB gauche de l'appareil UFED.

3) Sur l'unité UFED :

   a) Dans le **Menu principal**, sélectionnez une des options suivantes :

      - Pour une extraction numérique, sélectionnez **Extraction numérique**.
      - Pour une extraction de système de fichiers, sélectionnez **Extraction de système de fichiers**.

   b) Sélectionnez le fabricant de l'appareil dans le menu **Sélectionner le modèle**.

   c) Sélectionnez le modèle de l'appareil.

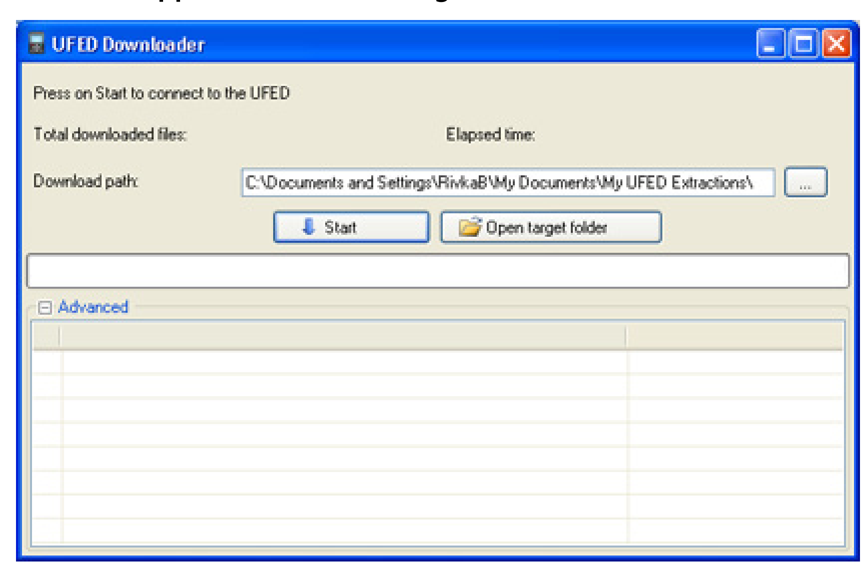
4) Sur le PC, cliquez sur **Démarrer** > **UFED Logical Analyzer** pour ouvrir UFED Logical Analyzer.

   L'application **UFED Logical Analyzer** s'ouvre.

5) Cliquez sur l'icône **Lire des données depuis UFED** dans la barre d'outils de l'application.



La fenêtre **Application de téléchargement UFED** s'ouvre.

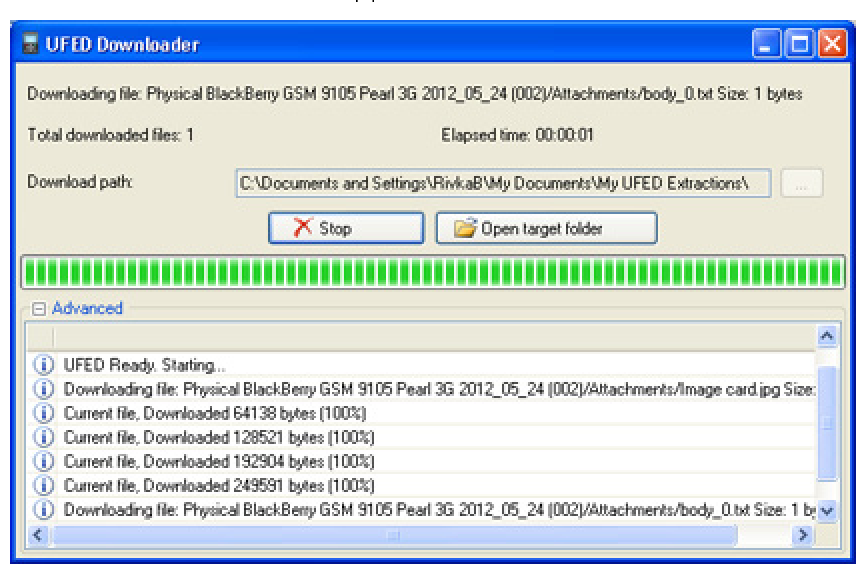


6) Dans le champ **Chemin de téléchargement**, cliquez sur [...] et choisissez l'emplacement souhaité pour l'extraction.

Conseil : Cliquez sur **Ouvrir le dossier cible** pour afficher le contenu du dossier cible sélectionné.

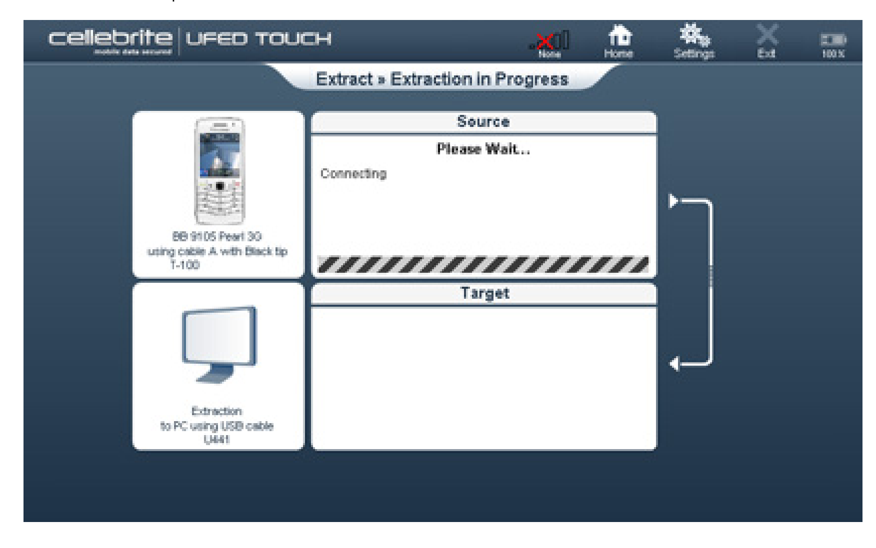
7) Sur l'unité UFED Touch, dans l'écran « Sélectionner l'emplacement de l'extraction », choisissez **PC**.
8) Suivez les invites sur l'unité UFED Touch jusqu'à ce qu'il vous soit demandé de lancer la procédure de téléchargement.
9) Sur le PC, dans UFED Logical Analyzer, cliquez sur **Démarrer** dans la fenêtre « Application de téléchargement UFED ».

Le transfert de données de l'appareil vers le PC commence.

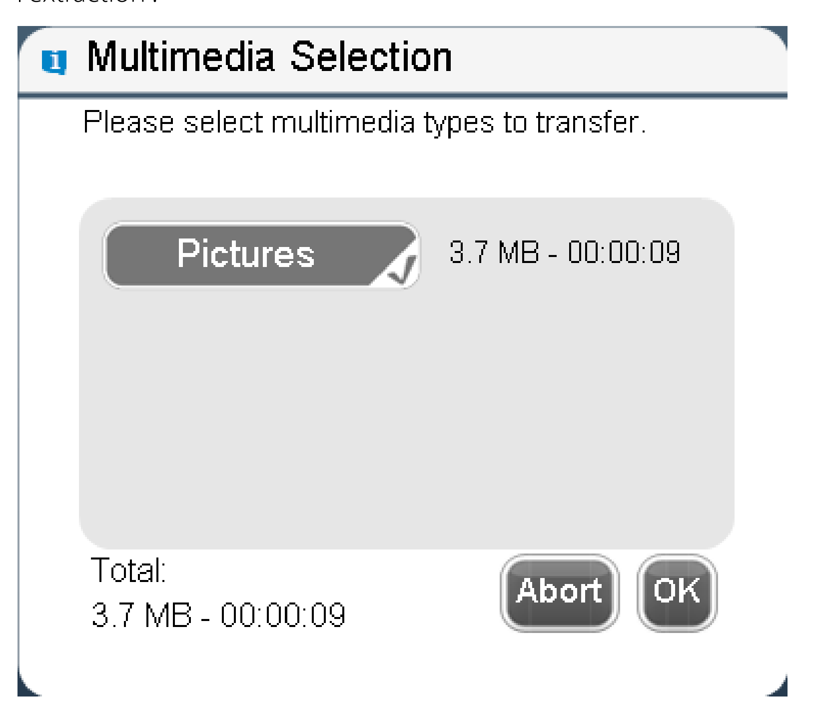




Au cours du processus d'extraction, l'écran « Extraction en cours » s'affiche sur l'unité UFED :



Sur l'unité UFED, vous êtes invité à sélectionner les types de fichiers multimédia à inclure dans l'extraction :



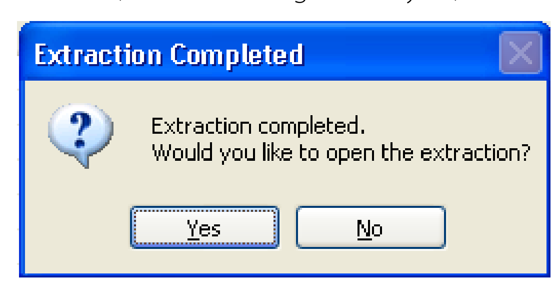


10) Assurez-vous que les types de fichiers multimédia que vous souhaitez inclure dans l'extraction sont marqué d'une ✓. Pour annuler l'extraction d'un type de fichier multimédia spécifique, cliquez sur ✓ sur le nom de celui-ci.

11) Cliquez sur **OK**.

Le processus d'extraction se poursuit. Lorsque le processus est terminé, la fenêtre **Résumé d'extraction du téléphone** s'affiche sur l'unité UFED Touch.

Sur le PC, dans UFED Logical Analyzer, le message suivant s'affiche :



12) Cliquez sur **Oui**.

L'extraction s'ouvre dans UFED Logical Analyzer, et l'écran « Résumé d'extraction » s'affiche.

3.4. Enregistrer une session de projet

Enregistrez la session de projet pour sauvegarder votre travail. Vous pourrez ainsi fermer UFED Logical Analyzer et reprendre votre session plus tard.

Le fichier de session (.pas) enregistré inclut :

- La sélection de l'utilisateur dans les tableaux **Données analysées** et **Fichiers de données**,
- Les signets d'entités,
- Les résultats de la liste de surveillance,
- Les onglets ouverts,
- Les rapports générés,
- Les paramètres temporels unifiés,
- Les paramètres d'informations du dossier.

Il est également possible de créer une session de projet pour les extractions effectuées par des outils tiers.

REMARQUE : Les sessions de projet enregistrées ne contiennent pas de paramètres définis. Pour en savoir plus sur comment enregistrer vos paramètres, consultez la section ***Enregistrer les paramètres*** (page ***184***).



Pour enregistrer une session de projet :

1) Dans le menu **Fichier**, sélectionnez **Enregistrer une session de projet**.

   La boîte de dialogue « Enregistrer sous » s'affiche.

2) Accédez à l'emplacement dans lequel vous souhaitez enregistrer le fichier de la session de projet.
3) Pour changer le nom du fichier, modifiez le nom attribué automatiquement dans la zone de texte **Nom du fichier**.

   REMARQUE : Pour remplacer une session précédente, choisissez le même nom de fichier.

4) Cliquez sur **Enregistrer**.

3.5. Charger une session de projet

1) Dans l'onglet **Accueil**, ouvrez le projet avec lequel vous souhaitez travailler.
2) Dans le menu **Fichier**, sélectionnez **Charger une session de projet**.
3) Dans la boîte de dialogue Ouvrir, accédez au fichier de session de projet que vous souhaitez ouvrir.
4) Cliquez sur **Ouvrir**.

   La session s'ouvre.

3.6. Fermer un projet

- Utilisez une des méthodes suivantes :
  - Dans le menu **Fichier**, sélectionnez **Fermer**.
  - Cliquez avec le bouton droit de la souris sur le nom du projet et sélectionnez **Fermer**.

3.7. Fermer UFED Logical Analyzer

- Dans le menu **Fichier**, sélectionnez **Quitter**.

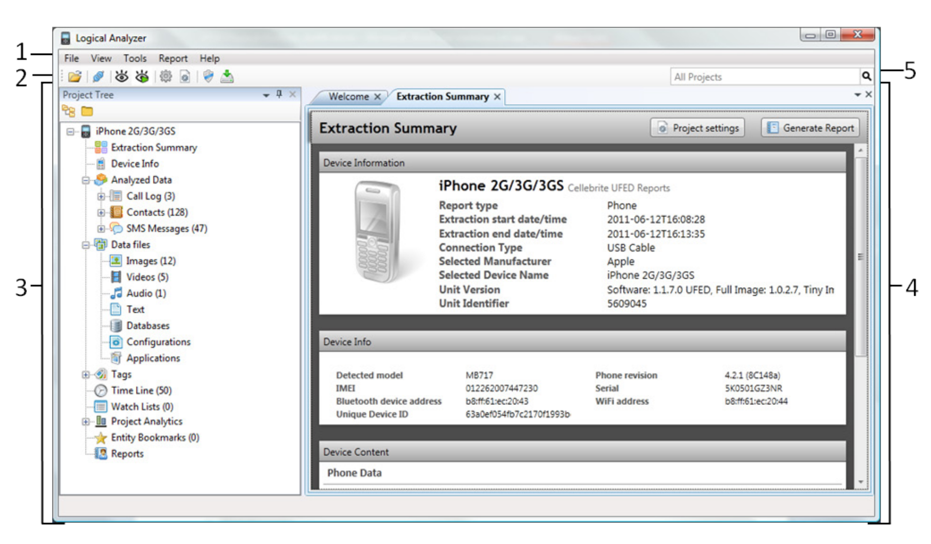


3.8. Raccourcis clavier

Ctr+O	Ouvrir un fichier
Ctr+W	Fermer un projet
Ctrl+P	Ouvrir les paramètres du projet
Ctrl+I	Ouvrir l'assistant iOS
Ctrl+T	Ouvrir les paramètres
Espace	Cocher ou décocher les cases
Ctrl+R	Ouvrir l'assistant de création de rapports
Ctrl+Tab	Passer d'un onglet ouvert à un autre
Ctrl+Début	Placer le curseur au début d'un tableau
Ctrl+Fin	Placer le curseur à la fin d'un tableau
Ctrl+B	Ajouter un signet d'entité
Ctrl+U	Ouvrir l'application de téléchargement UFED pour se connecter à UFED

Chapitre 4 : **S'orienter dans l'espace de travail**

L'espace de travail se compose de deux zones principales : l'arborescence de projet et la zone d'affichage des données permettant de simplifier votre travail.





L'espace de travail comprend les composants suivants :

1) Barre de menu de l'application
2) Barre d'outils de l'application
3) Arborescence de projet
4) Zone d'affichage de données
5) Recherche dans tous les projets

4.1. Arborescence de projet

La zone **Arborescence de projet** affiche la structure des informations extraites suivante pour chaque projet ouvert, pour analyse :

Élément de l'arborescence	Description
Résumé d'extraction	• Double-cliquez sur **Résumé d'extraction** pour ouvrir un résumé du projet dans la zone d'affichage des données. Pour plus d'informations, consultez l'onglet ***Résumé d'extraction*** (page ***60***).

Élément de l'arborescence	Description
Infos appareil	• Double-cliquez sur **Infos appareil** pour ouvrir un onglet dans la zone d'affichage des données. L'onglet **Infos appareil** fournit une liste des informations existantes, ainsi que des identifiants importants pour l'appareil, notamment les codes de carte SIM et de verrouillage de l'utilisateur, le cas échéant. Le nombre de catégories et la quantité d'informations affichées varie en fonction du modèle et du fabricant de l'appareil.



Élément de l'arborescence	Description
Données analysées	L'élément d'arborescence **Données analysées** affiche les groupes de données analysées correspondant à des fonctionnalités spécifiques de l'appareil, telles que les contacts, les SMS, les journaux d'appel, etc. Les informations disponibles et ce qui s'affiche varient en fonction des fonctionnalités de l'appareil, du contenu et de la version de l'application. Par exemple, les SMS sont triés en fonction des dossiers utilisés par la fonctionnalité de messagerie de l'appareil (Brouillons, Reçus, Envoyés, etc.). Les e-mails sont triés en fonction du compte de messagerie avec lequel ils ont été envoyés ou reçus. Un dossier « Non classés » contient les messages qui ne peuvent être classés dans aucun des comptes ou dossiers de compte trouvés (Brouillons, Reçus, Envoyés, etc.). Les types d'informations suivants peuvent s'afficher dans les **Données analysées** : • Informations personnelles : calendrier, contacts, notes, journal d'appels, dictionnaires utilisateur, comptes utilisateur ;

Élément de l'arborescence	Description
	• Éléments de messagerie : SMS, MMS, e-mails, messages instantanés, chat ; Le nombre entre parenthèses indique le nombre d'éléments que contient chaque catégorie.



Élément de l'arborescence	Description
Fichiers de données	L'élément d'arborescence **Fichiers de données** trie les données extraites en formats de fichier communs ou connus, utilisés par les appareils et ordinateurs : images, vidéos, fichiers audio ou fichiers texte. Dans l'arborescence de projet, les informations affichées sont triées selon les catégories suivantes : • **Images** - Fichiers reconnus comme des fichiers image • **Vidéos** - Fichiers reconnus comme des fichiers vidéo • **Audio** - Fichiers reconnus comme des fichiers audio • **Texte** - Fichiers reconnus comme des fichiers texte • **Bases de données** - Structures de données reconnues comme des bases de données • **Applications** – Fichiers reconnus comme des fichiers d'application (fichiers .apk, .jar, .dex, .so, .exe, etc.)

Élément de l'arborescence	Description
	• **Documents** – Fichiers reconnus comme des fichiers documents (fichiers .doc, .docx, .pdf, .xlsx, .ppt, etc.) Vous pouvez créer des groupes de fichiers de données supplémentaires. Pour plus d'informations, consultez la section ***Gérer les paramètres des fichiers de données*** (page *168*).
Balises	Certains types de fichiers sont identifiés et balisés dans les données extraites. Il existe huit balises par défaut : **Applications**, **Audio**, **Configurations**, **Bases de données**, **Documents**, **Images**, **Texte** et **Vidéos**.
Chronologie	• Double-cliquez sur **Chronologie** pour ouvrir les événements de l'appareil organisés par ordre chronologique dans la zone d'affichage des données. L'onglet **Chronologie** affiche les événements horodatés de l'appareil : appels, SMS, MMS, etc. dans une vue séquentielle.



Élément de l'arborescence	Description
Listes de surveillance	Les listes de surveillance sont des listes de mots clés que vous créez et utilisez pour rechercher et identifier des événements et éléments spécifiques dans les données extraites. • Développez les **Listes de surveillance** pour afficher une liste des listes de surveillances exécutées au cours de la session actuelle. Pour plus d'informations, consultez la section ***Travailler avec les listes de surveillance*** (page ***86***).
Des signets d'entités	Les signets d'entités que vous créez sont gérés dans la section **Signets d'entités** de l'arborescence du projet. Le nombre de signets d'entités du projet apparaît entre parenthèses à côté du nom de la section. • Double-cliquez sur **Signets d'entités** pour ouvrir une liste des signets d'entités dans un onglet dans la zone d'affichage des données.

Élément de l'arborescence	Description
	• Double-cliquez sur un signet d'entité pour aller à l'élément marqué dans l'onglet d'affichage correspondant. Par exemple, double-cliquez sur un signet d'entité correspondant à un SMS pour ouvrir la liste de SMS dans un onglet d'affichage des Données analysées, avec l'élément marqué mis en surbrillance. Pour plus d'informations, consultez la section ***Informations sur les signets (signets d'entités)*** (page ***99***).
Rapports	Pour ouvrir un rapport qui a déjà été créé pour le projet : • Double-cliquez sur le rapport dans l'élément d'arborescence **Rapports**. Le rapport s'ouvre dans l'application associée au format du rapport.



Élément de l'arborescence	Description
	• Si aucun rapport n'a été créé pour le projet, double-cliquez sur l'élément d'arborescence **Rapports** pour ouvrir la boîte de dialogue Générer un rapport. Pour en savoir plus sur la création d'un rapport, consultez la section Générer un rapport.
Analyse de projet	L'élément d'arborescence **Analyse de projet** fournir une présentation de l'analyse comparative. Vous pouvez ouvrir un onglet Analyse d'activité pour afficher une présentation de la totalité de l'activité de l'appareil, ainsi que des onglets correspondants aux activités du téléphone, des e-mails, de WhatsApp, de Skype, de Gmail et de BlackBerry Messenger. Pour plus d'informations, consultez la section ***Définir les paramètres du projet*** (page *185*).

4.1.1. Travailler dans la zone Arborescence de projet

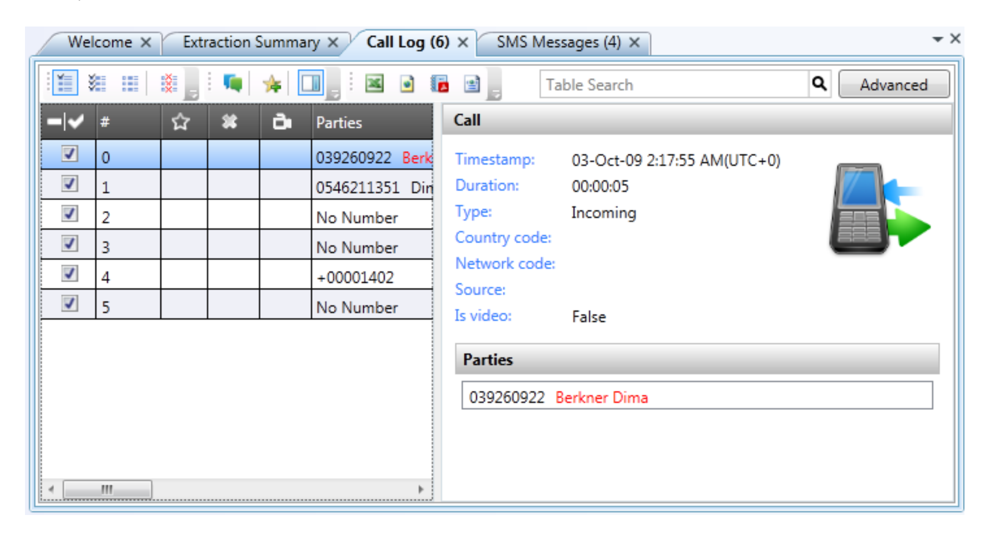
Ouvrez les éléments d'arborescence pour étudier et localiser des informations spécifiques :

- Cliquez pour développer ou pour réduire les éléments de l'arborescence.
- Double-cliquez sur un élément de l'arborescence pour ouvrir les informations détaillées dans la zone d'affichage des données.
- Cliquez sur en haut de l'arborescence du projet pour développer tous les éléments de celle-ci.
- Cliquez sur en haut de l'arborescence du projet pour réduire tous les éléments de celle-ci.



4.2. Zone d'affichage de données

Double-cliquez sur un élément pour l'afficher dans un onglet. Un nouvel onglet est ouvert pour chaque élément.



Il existe quatre types d'onglet :

- Onglet **Accueil**.
- Onglet **Résumé d'extraction**.
- Onglets de données, avec sous-onglets qui présentent une vue particulière, en fonction des données.
- Onglet **Chronologie**.

La zone d'affichage de données affiche également des fenêtres supplémentaires telles que la fenêtre Trace, la vue Chronologie et les résultats de la liste de surveillance.

Pour fermer un onglet :

- Utilisez une des méthodes suivantes :
  - Cliquez sur X sur l'en-tête de l'onglet.
  - Cliquez sur X dans l'angle supérieur droit de la zone d'affichage des données.

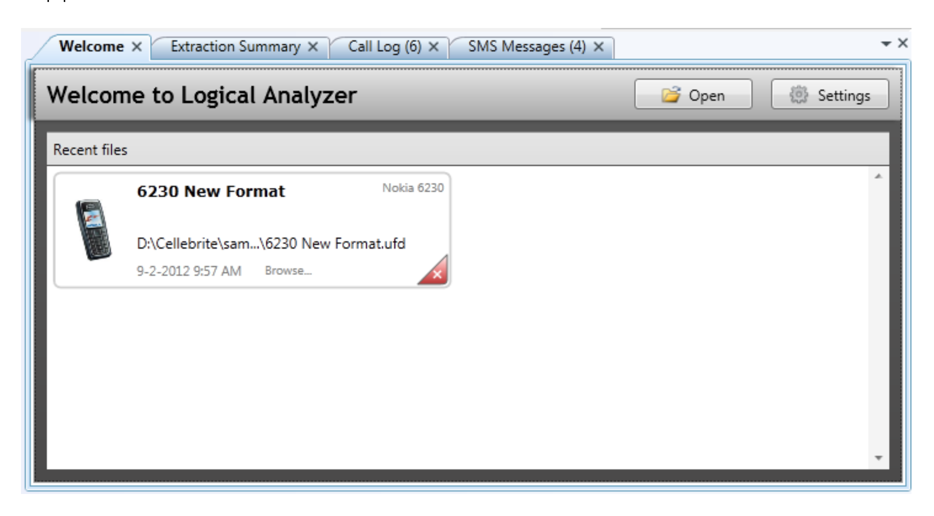
Pour accéder à un onglet spécifique :

- Dans l'angle supérieur droit de la zone d'affichage de données, cliquez sur ▼, puis sélectionnez l'onglet souhaité dans la liste des onglets ouverts.



4.2.1. Onglet Accueil

L'onglet **Accueil** apparaît automatiquement dans la zone d'affichage des données au lancement de l'application. Il affiche une liste des fichiers ouverts récemment.



Chaque fichier dans la liste s'affiche sous la forme d'un groupe d'informations encadrées qui contient les éléments suivants :

- Image de l'appareil : image miniature de l'appareil tirée des ressources de l'application, lorsqu'elle est disponible. Lorsqu'aucune image n'est disponible, une image générique est utilisée.
- Nom du fichier : nom du fichier ouvert, sans l'extension.
- Chemin du fichier : chemin système vers le fichier.
- Modèle de l'appareil : fabricant et modèle de l'appareil identifié, ou « BINARY » si le fichier ouvert est une extension binaire.
- Nom du dossier : si un nom de dossier a été attribué au rapport, celui-ci s'affiche ici. Le nom peut être défini dans les paramètres du projet.
- Date et heure : date et heure de la dernière ouverture du fichier.
- Lien de navigation : lien direct vers le fichier dans le système.
- Supprimer élément récent : cliquez ici pour supprimer l'élément de l'onglet **Accueil**.

Vous pouvez procéder de la façon suivante :

- Cliquez sur un élément encadré pour ouvrir les fichiers à décoder.
- Cliquez sur **Parcourir** pour accéder directement au fichier associé dans le système de fichiers.
- Fermez l'onglet **Accueil**. Pour l'ouvrir à nouveau, allez dans **Vue** > **Afficher Accueil**.



4.2.2. Onglet Résumé d'extraction

L'onglet **Résumé d'extraction** s'affiche automatiquement lorsque vous ouvrez une nouvelle extraction pour analyse.

Welcome × | Extraction Summary × | SMS Messages (47) ×

Extraction Summary — Project settings — Generate Report

Device Information

iPhone 2G/3G/3GS Cellebrite UFED Reports

Report type	Phone
Extraction start date/time	2011-06-12T16:08:28
Extraction end date/time	2011-06-12T16:13:35
Connection Type	USB Cable
Selected Manufacturer	Apple
Selected Device Name	iPhone 2G/3G/3GS
Unit Version	Software: 1.1.7.0 UFED, Full Image: 1.0.2.7, Tiny In
Unit Identifier	5609045

Device Info

Detected model	MB717	**Phone revision**	4.2.1 (8C148a)
IMEI	012262007447230	**Serial**	5K0501GZ3NR
Bluetooth device address	b8:ff:61:ec:20:43	**WiFi address**	b8:ff:61:ec:20:44
Unique Device ID	63a0ef054fb7c2170f1993b		

Device Content

Phone Data

- Pour rouvrir l'onglet lorsqu'il est fermé, double-cliquez sur l'élément d'arborescence **Résumé d'extraction**.

L'onglet **Résumé d'extraction** peut afficher les informations suivantes :

- **Informations de l'extraction** : informations relatives à l'extraction de l'appareil. Telles que :

Date/heure début d'extraction *Date/heure fin d'extraction*	Début et fin de l'extraction.
Identifiant d'unité	Numéro de série de l'appareil qui a effectué l'extraction (par ex. UFED Touch), ou un identifiant unique si l'extraction a été effectuée par une application PC (par ex. UFED 4PC).
Version d'unité	Version du logiciel UFED (par ex. 4.1.0.220)
Fabricant sélectionné	Fabricant de l'appareil (par ex. Apple)
Nom d'appareil sélectionné	Nom de l'appareil (par ex. iPhone 4)
Type de connexion	Câble utilisé pour l'extraction (par ex. Câble n° 100)
Type d'extraction	Type d'extraction effectué (par ex. numérique)
ID d'extraction	ID unique pour chaque type d'extraction

- **Infos appareil** : résumé des informations spécifiques de l'appareil tirées du fichier d'extraction. Consultez l'élément *Infos appareil* dans ***Arborescence de projet*** (page ***46***).



- **Contenu de l'appareil** : contenu analysé, divisé en catégories :
  - **Données du téléphone** : type de données de l'appareil analysées trouvées lors de l'extraction (journal d'appels, contacts, SMS, etc.). Pour une liste complète des types de données de téléphone, consultez l'élément *Données analysées* dans ***Arborescence de projet*** (page ***46***).
  - **Fichiers de données** : type de fichiers de données standard trouvées lors de l'extraction (images, vidéos, fichiers audio et fichiers texte). Consultez la section ***Fichiers de données*** (page ***165***).

Pour afficher les informations correspondantes dans un nouvel onglet dans la zone d'affichage des données :

- Cliquez sur un élément de l'arborescence.

4.2.3. Onglets de données

Les onglets de données affichent les fichiers d'un type spécifique (journal d'appels, contacts, SMS, etc.).

Chaque type de fichier de données dispose de plusieurs modes d'affichage des données :

Fichiers images	**Vue image** et **Infos fichier**
Fichiers vidéo	**Infos fichier**
Fichiers audio	**Infos fichier**
Fichiers de texte	**Infos fichier**
Bases de données	**Vue base de données et Infos fichier**
Fichiers documents	**Infos fichier**

Les onglets de données affichent les données dans plusieurs sous-onglets, selon le type de données :

- **Vue texte** : affiche les fichiers texte sous forme de texte.



- **Vue tableau** : liste de tous les fichiers d'un type spécifique (images, vidéos, fichiers audio, fichiers texte, etc.) trouvés au cours du processus d'analyse de données.
- **Vue dossier** : affiche la structure de dossiers des chemins des fichiers de données dans le système de fichiers reconstruit (pour les fichiers de données uniquement).
- **Vue image** : affiche l'image. Consultez la section ***Afficher les fichiers image*** (page *71*).
- **Vue miniature** : affiche des miniatures des images (pour les images uniquement).
- **Infos fichier** : affiche les informations relatives au fichier.

4.2.3.1. Travailler dans les onglets de données

Sélectionner des éléments :

Sélectionnez les éléments dans la zone d'affichage des données pour les inclure dans un rapport que vous créez. Par défaut, tous les éléments sont sélectionnés.

- Pour sélectionner plusieurs éléments, maintenez la touche MAJ ou CTRL (pour une sélection consécutive ou non consécutive, respectivement).
- Lorsqu'un élément est sélectionné, appuyez sur la barre d'espace pour cocher ou décocher la case, afin d'indiquer si l'élément doit être inclus ou exclus du rapport.
- Pour sélectionner tous les éléments, cochez la case dans l'en-tête de la colonne (vue tableau et chronologie) ou cochez la case **Tout sélectionner** (vue miniature).

Trier les colonnes :

Vous pouvez trier chaque colonne par ordre alphabétique ou chronologique.

- Cliquez sur l'en-tête de la colonne pour modifier l'ordre de tri.

Réorganisation des colonnes :

Vous pouvez modifier l'ordre des colonnes à votre convenance. Votre préférence sera conservée pour la durée de la session.

- Faites glisser chaque colonne jusqu'à l'emplacement souhaité.

Afficher ou masquer les colonnes :

- Cliquez avec le bouton droit de la souris sur l'en-tête de la colonne et sélectionnez le nom de la colonne dans la liste.

Afficher des informations supplémentaires :

Pour les onglets de données qui contiennent des informations sous forme de texte, le panneau de droite est ouvert par défaut, et affiche les informations relatives à l'élément sélectionné.

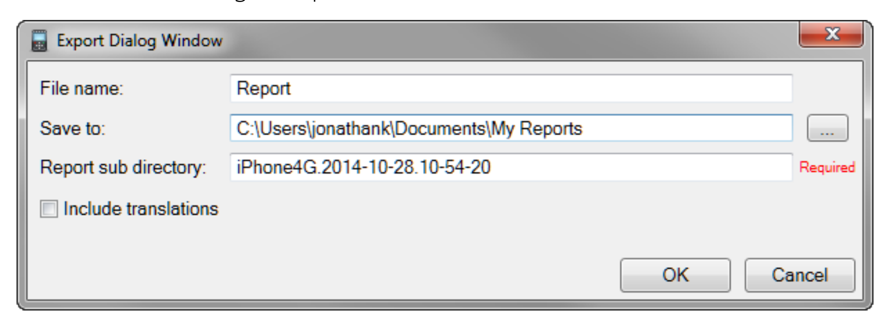
- Pour ouvrir ou fermer le panneau de droite, cliquez sur .



Exporter des données :

1) Pour exporter des données vers un onglet spécifique, cliquez sur le format souhaité dans la barre d'outils : Excel , HTML , PDF , XML , KML (données de positionnement uniquement) ou EML (données d'e-mail uniquement).

La fenêtre de dialogue Exporter s'affiche.



2) Utilisez une des méthodes suivantes :
   - Saisissez le chemin de l'emplacement où vous souhaitez sauvegarder le rapport.
   - Cliquez sur ... et sélectionnez l'emplacement souhaité.
3) Cochez la case **Inclure les traductions** pour inclure les données traduites.
4) Cliquez sur **OK**.

Le rapport est créé, et un message s'affiche, vous demandant si vous souhaitez l'ouvrir avec un logiciel tiers.

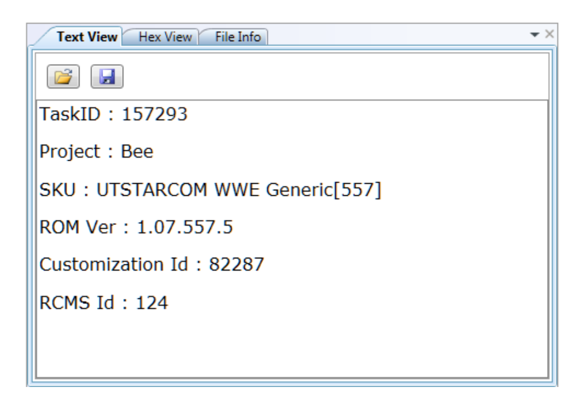
5) Cliquez sur **Oui** ou **Non**.

Le fichier s'ouvre avec le logiciel tiers par défaut.

REMARQUE : Lorsque vous exportez un rapport au format EML, un fichier est créé pour chaque e-mail.

4.2.3.2. Vue texte

Pour les fichiers de données composés de texte, affichez les données dans un fichier texte.





4.2.3.3. Vue tableau pour les fichiers de données

Pour les fichiers de données, le tableau affiche les informations suivantes :

	Indique si l'élément doit être inclut (coché) ou exclu (décoché) dans le rapport généré.
N°	Numéro de ligne.
	Indique si l'élément est marqué par un signet.
	Indique si le fichier de données a été supprimé , ou si son état est inconnu (« ? » ou icône de document blanche).
Image	Une miniature de l'image ou une icône du type de fichier. (Fichiers de données image uniquement).
Nom	Nom du fichier.
Chemin	Chemin racine du fichier de données.

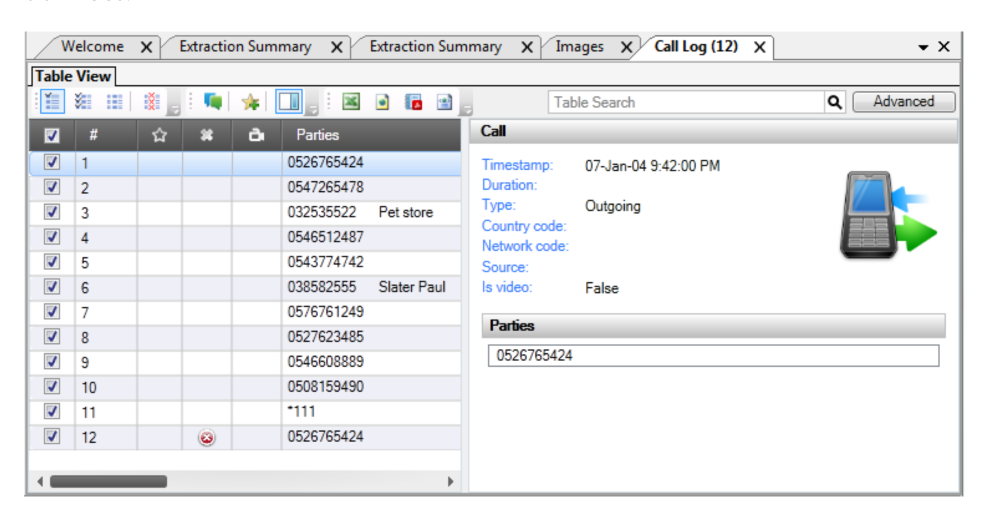
Taille	Taille du fichier.
Métadonnées	Métadonnées supplémentaires du fichier de données.
Date de création	Horodatage de création du fichier de données.
Modifié	Horodatage de modification du fichier de données.
Date d'accès	Horodatage du dernier accès au fichier de données.
Note de signet	Détails du signet.

En outre, des indicateurs s'affichent pour montrer les pièces jointes, indiquer les appels vidéo et même les directions.



4.2.3.4. Vue tableau pour les données analysées

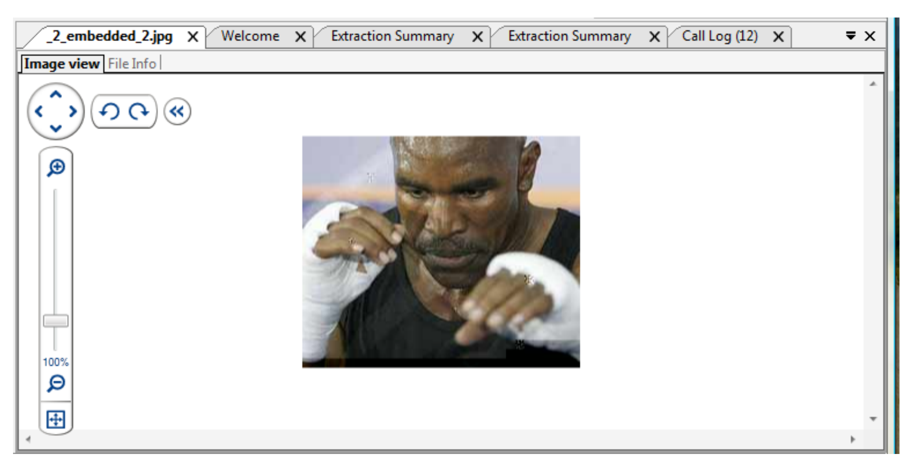
Pour les données analysées, les onglets Vue tableau affichent une liste de tous les événements d'un type spécifique (journal d'appels, contacts, SMS, etc.) trouvés au cours du processus d'analyse de données.



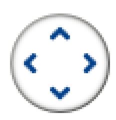
4.3. Afficher les fichiers image

1) Double-cliquez sur une image dans un onglet d'affichage des données.

   Un nouvel onglet contenant l'image s'ouvre. Cet onglet est divisé en deux sous-onglets : **Vue image** et **Infos fichier**.



2) Dans l'onglet **Vue image**, utilisez les commandes de l'image :



Parcourir l'image, lorsqu'elle est agrandie.

 Faire pivoter l'image dans le sens des aiguilles d'une montre et dans le sens inverse.

 Zoom avant et arrière. Vous pouvez également ajuster le zoom à l'aide de la barre de glissement.

 Faire un zoom avant pour ajuster l'image à l'onglet.

 Redéfinir un zoom de 100 %.

 Masquer les commandes de l'image.

3) Cliquez sur l'onglet **Infos fichier** pour afficher les informations relatives au fichier. Par exemple, la section Métadonnées de fichier inclut des informations telles que l'Heure de capture, qui correspond à la date et l'heure auxquelles la photo a été prise.

4.4. Lire des fichiers vidéo

Pour lire des fichiers vidéo avec UFED Logical Analyzer :

1) Dans le tableau de données, double-cliquez sur le fichier média que vous souhaitez lire.

   Un nouvel onglet s'ouvre pour le fichier média.

2) Cliquez sur .

Pour lire la vidéo avec le programme par défaut :

- Cliquez avec le bouton droit de la souris sur le fichier média et sélectionnez **Ouvrir avec le programme par défaut**.


cellebrite
delivering mobile expertise

Chapitre 5 : **Localisation et analyse des informations**

Cette section décrit comment parcourir, rechercher, filtrer, marquer par un signet et gérer les informations dans votre projet.

5.1. Rechercher des informations dans un onglet de données

Dans les onglets **Vue tableau**, recherchez un élément particulier dans le tableau de données. La recherche est effectuée sur toutes les entrées de données du tableau.

- Dans la case **Rechercher dans le tableau**, saisissez la chaîne de votre choix.

  Le tableau est mis à jour pour afficher uniquement les éléments qui contiennent la chaîne que vous avez saisie.



5.2. Utiliser le filtre rapide

Utilisez les outils du filtre rapide pour filtrer les données dans les onglets **Vue tableau** de la façon suivante :

	Tout afficher	Affiche tous les éléments.
	Sélectionné uniquement	Affiche les éléments sélectionnés.
	Non sélectionné uniquement	Affiche les éléments non sélectionnés.
	Supprimé	Affiche les éléments supprimés.
	Tout afficher	Affiche toutes les images.
	Afficher les images de plus de 30 Ko	Affiche uniquement les petites images de plus de 30 Ko.
	Afficher les images de plus de 100 Ko	Affiche uniquement les images de taille moyenne de plus de 100 Ko.

	Afficher les images de plus de 500 Ko	Affiche les grandes images uniquement (plus de 500 Ko).
	Filtrer les images (par extension)	Cliquez ici pour activer le filtre par type de fichier.
	Afficher les fichiers JPEG	Affiche les fichiers JPG ou JPEG.
	Afficher les fichiers GIF	Affiche les fichiers GIF.
	Afficher les fichiers BMP	Affiche les fichiers BMP.
	Afficher les fichiers PNG	Affiche les fichiers PNG.
	Filtre métadonnées	Filtrez les fichiers image et vidéo par métadonnées (Toutes, Sans métadonnées ou Contient des métadonnées) et par emplacement (Tous, Possède un emplacement ou Sans emplacement).



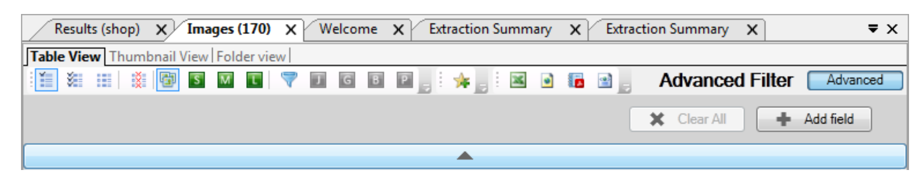
	Filtre heure de capture	Filtrez les fichiers image et vidéo en fonction de l'heure de capture. La plage maximum est affichée par défaut, et vous pouvez sélectionner une plage spécifique définie par une date et une heure.
	Filtre traduction	Filtrez le texte traduit pour afficher tout le texte, le texte traduit ou le texte non traduit.

REMARQUE : Les éléments de la barre d'outils varient selon le contexte, et s'affichent uniquement lorsque des données pertinentes sont affichées.

5.3. Utiliser le filtre avancé

Utilisez le filtre avancé pour filtrer la liste selon plusieurs paramètres.

1) Dans la barre d'outils du filtre, cliquez sur **Avancé**.



2) Cliquez sur **Ajouter un champ**, puis sélectionnez un champ dans la liste déroulante. La liste de champs se compose des colonnes dans l'onglet de données actuel.
3) Dans la case qui s'affiche pour le champ sélectionné, saisissez la chaîne ou l'horodatage de votre choix.

   L'onglet affiche uniquement les éléments correspondant au filtre.

4) Pour ajouter d'autres filtres, répétez les étapes 2 et 3.

   Lorsque vous ajoutez des filtres dans la recherche avancée, les résultats correspondent à tous les critères spécifiés.

5) Pour effacer la chaîne saisie, cliquez sur ✖.
6) Pour effacer toutes les chaînes saisies, cliquez sur **Tout effacer**.



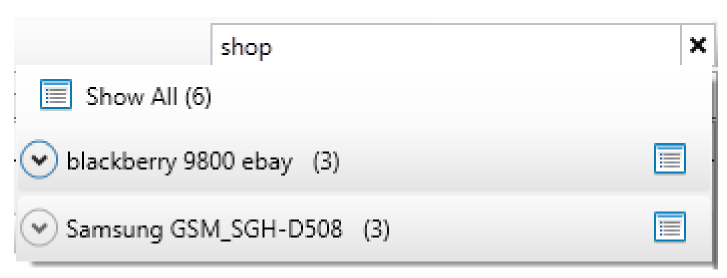
7) Pour supprimer le filtre du champ, cliquez sur .
8) Pour fermer le filtre avancé, cliquez sur **Avancé**.

5.4. Rechercher des informations dans tous les projets ouverts

Utilisez la boîte de recherche **Tous les projets** dans la barre d'outils pour rechercher des informations dans tous les projets ouverts.

1) Saisissez la chaîne de votre choix dans la case **Tous les projets**.

   Une liste des résultats correspondants s'affiche sous le champ de recherche **Tous les projets**. Les résultats sont triés par projet ouvert. Dans chaque projet, les résultats sont triés par catégories, selon le type (SMS, messages, contacts, fichiers, etc.). Le nombre de résultats dans chaque catégorie type s'affiche également.



2) Cliquez sur pour réduire ou développer les projets.
3) Utilisez une des méthodes suivantes :
   - Cliquez sur à côté du nom d'un projet pour afficher les résultats de la recherche dans cette extraction dans un onglet, dans la zone d'affichage des données.
   - Sélectionnez **Tout afficher** en haut de la liste de résultats rapides pour afficher un onglet Résultats dans la zone d'affichage des données montrant tous les résultats de la recherche. La chaîne correspondante dans chaque élément apparaît en rouge.
     Comme dans la liste de résultats rapides, l'onglet Résultats répertorie les résultats par type.

5.5. Vue Chronologie

La vue Chronologie est un outil puissant qui vous permet d'analyser les données dans l'ordre chronologique, afin d'identifier l'ordre des événements et d'établir des liens entre eux.

La vue Chronologie dispose de deux affichages : tableau et graphique.



Dans la vue tableau, les événements apparaissent dans un tableau, classés par date et heure.

Welcome × | Extraction Summary × | Time Line (3521) ×

Table View | Graphic View

Table Search | Advanced

#	Type	Timestamp
3/21/2011 (1)		
1	IP Connections	21/03/2011 13:03:37(L
5/16/2011 (13)		
2	Installed Applications	16/05/2011 08:57:21(L
3	Instant Messages	16/05/2011 09:02:29(L
4	Instant Messages	16/05/2011 09:02:53(L
5	Call Log	16/05/2011 09:05:27(L
6	Instant Messages	16/05/2011 09:06:18(L
7	Instant Messages	16/05/2011 09:06:24(L
8	Instant Messages	16/05/2011 09:06:26(L
9	Instant Messages	16/05/2011 09:06:28(L
10	SMS Messages	16/05/2011 10:59:12(L
11	SMS Messages	16/05/2011 10:59:15(L
12	SMS Messages	16/05/2011 10:59:50(L
13	SMS Messages	16/05/2011 11:00:04(L
14	SMS Messages	16/05/2011 11:01:12(L
5/22/2011 (103)		
15	Locations	22/05/2011 13:30:41(L
16	Locations	22/05/2011 13:30:42(L

IP Connection

Domain:
Router Address: 192.168.3.1
MAC Address: 00:1E:E5:45:AD:92
Cellular WAN:
Timestamp: 21/03/2011 13:03:37 (UTC +0)
Service Name:

Device IP

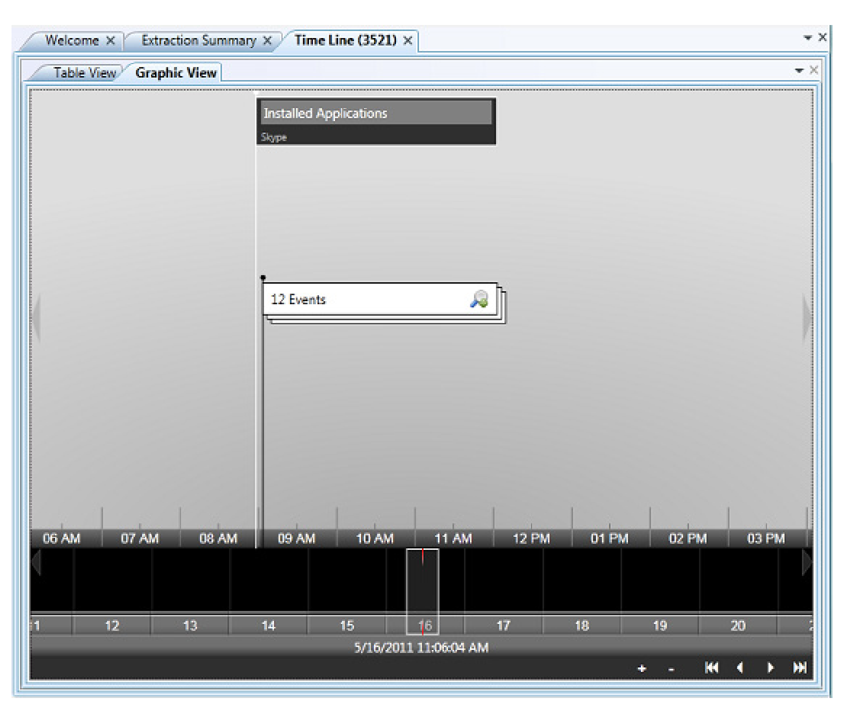
192.168.3.140

DNS Addresses

192.168.3.1

- Cliquez sur pour regrouper ou séparer les événements en fonction de la date.

Dans la vue graphique, les événements apparaissent dans un graphique. Cela vous permet d'identifier rapidement les pics d'activité potentiellement intéressants.





- Pour avancer ou reculer dans la chronologie, utilisez les boutons , , et .

Vous pouvez augmenter ou réduire le niveau de détail de la vue Chronologie :

- Pour augmenter la résolution temporelle, cliquez sur .
- Pour réduire la résolution temporelle, cliquez sur .

Les événements qui se produisent à peu d'intervalle sont marqués par groupes.

- Cliquez sur pour ouvrir un autre onglet Vue chronologie pour un groupe d'événements.

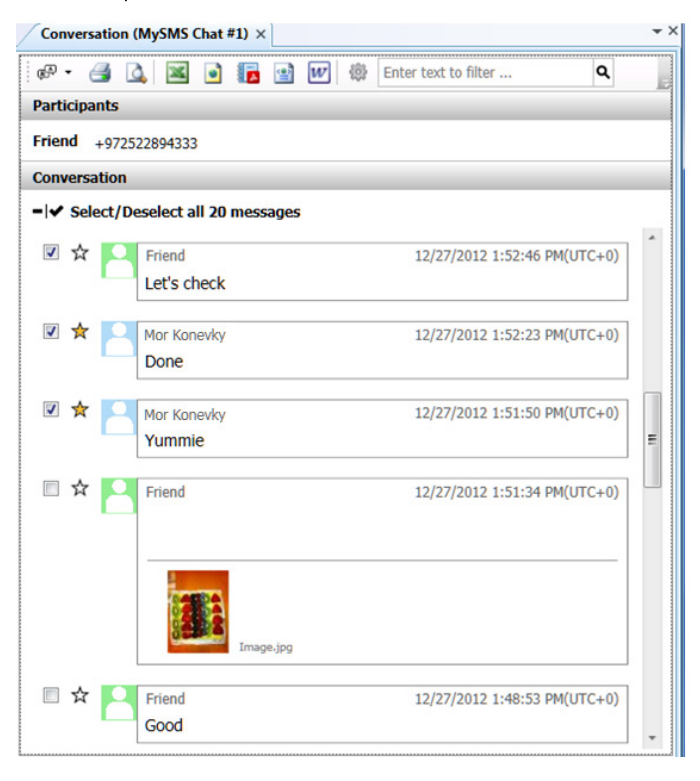
5.6. Accéder à la vue Conversation

Les données relatives aux communications (journaux d'appels, e-mails, SMS, MMS, etc.) peuvent être affichées dans une vue Conversation afin de suivre plus facilement et plus efficacement les communications entre deux parties ou plus. Vous pouvez rechercher des messages dans une conversation, sélectionner les messages à inclure dans un rapport (par défaut tous les messages de la conversation sont inclus), imprimer ou exporter la conversation.

Pour accéder à la vue Conversation et l'utiliser :

1) Dans un tableau de données relatives aux communications, sélectionnez l'un des enregistrements.
2) Cliquez sur .

Un onglet Conversation s'ouvre, affichant les éléments correspondants sous forme de conversation entre l'expéditeur et le destinataire de l'élément sélectionné.





3) Pour traduire ou supprimer le texte traduit, cliquez sur et sélectionnez **Tout traduire** ou **Supprimer toutes les traductions**.
4) Pour imprimer la conversation, cliquez sur .
5) Pour afficher un aperçu avant impression, cliquez sur .
6) Pour exporter la conversation, cliquez sur le format souhaité dans la barre d'outils de l'onglet Conversation : Excel , HTML , PDF , XML ou Word .
7) Pour modifier l'ordre de la conversation, cliquez sur et sélectionnez **Message le plus ancien en premier** ou **Message le plus récent en premier**.
8) Pour filtrer les messages, saisissez le texte dans la zone de recherche.
9) Pour ajouter ou modifier des signets, cliquez sur .
10) Cochez une case pour inclure des messages spécifiques dans le rapport (ou sélectionnez Tous les messages ou Aucun message).

5.7. Travailler avec les listes de surveillance

Exécutez une liste de surveillance composée de mots-clés sur vos données extraites afin d'identifier et de mettre en évidence les informations importantes et pertinentes.

La recherche par liste de surveillance peut être activée automatiquement ou exécutée manuellement sur les données décodées sélectionnées.

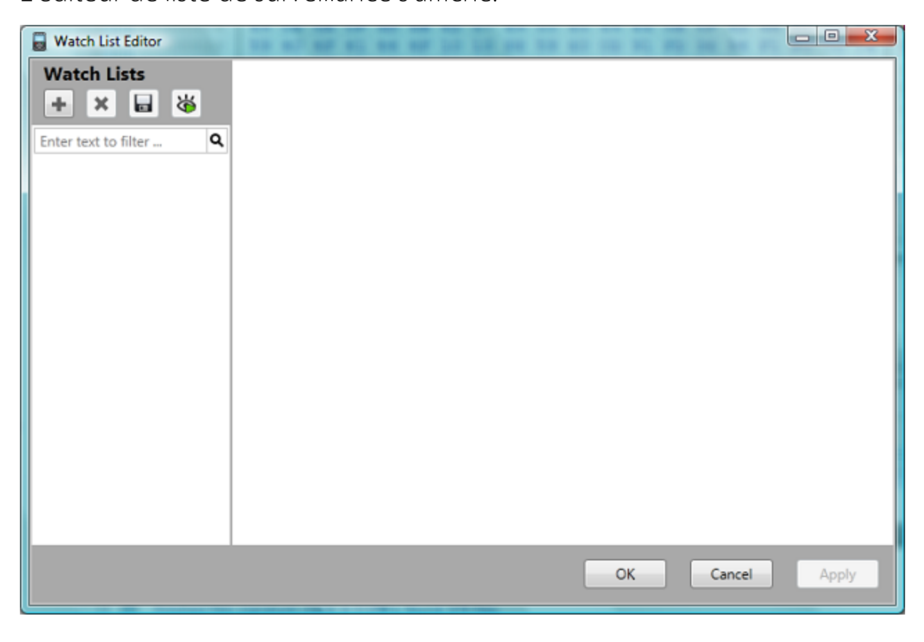
5.7.1. Créer une liste de surveillance

1) Utilisez une des méthodes suivantes :

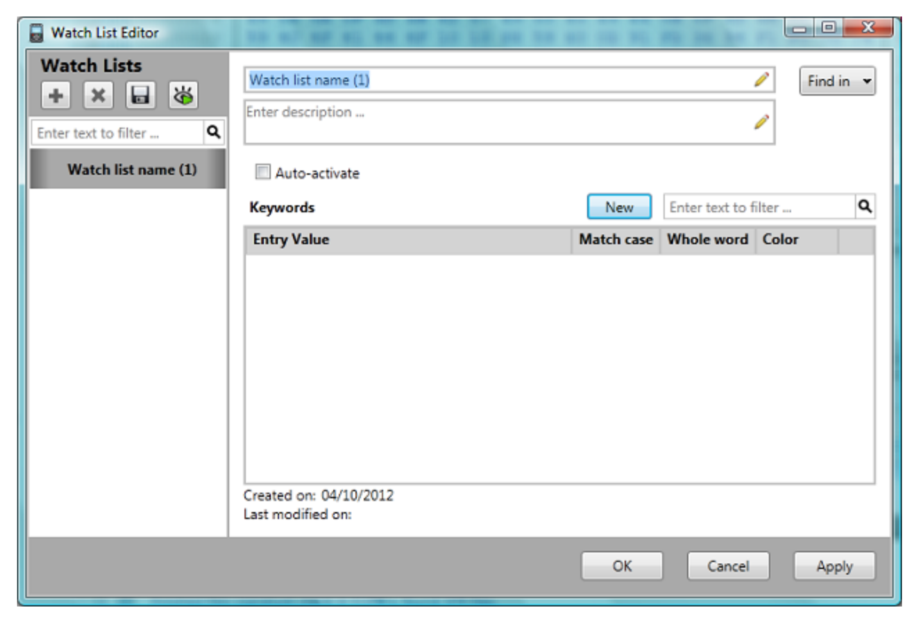
- Dans la barre d'outils, cliquez sur .
- Dans le menu **Outils**, sélectionnez **Éditeur de liste de surveillance**.



L'éditeur de liste de surveillance s'affiche.



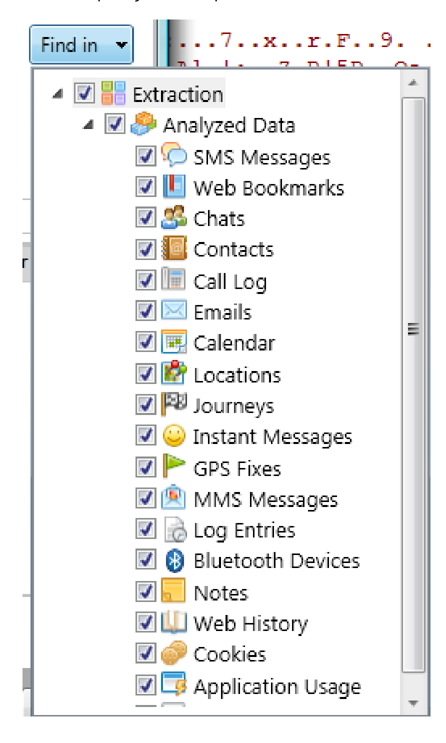
2) Cliquez sur [+], et sélectionnez **Nouveau**.



3) Dans la case **Nom de la liste de surveillance**, saisissez le nom de la liste.



4) Pour que la liste de surveillance recherche les mots-clés uniquement dans les types de données dans le projet, cliquez sur **Rechercher dans**, puis sélectionnez les types de données souhaités.



Lorsque vous exécutez la liste de surveillance, seuls les types de données sélectionnés sont consultés pour y rechercher des correspondances.

5) Dans la case **Saisir une description**, saisissez une description générale de la liste de surveillance (facultatif).
6) Pour que la liste de surveillance soit exécutée automatiquement lorsque vous ouvrez un projet, cliquez sur **Activation auto**.
7) Cliquez sur **Nouveau** pour ajouter un mot-clé.

   Une ligne avec le nouveau mot-clé apparaît dans la liste des mots-clés.

8) Pour chaque mot-clé, définissez les options suivantes, à votre convenance :
   - **Valeur d'entrée** : Saisissez le mot clé.
   - **Respecter la casse** : Sélectionnez cette option pour respecter la casse du mot-clé.
   - **Mot entier** : Sélectionnez cette option pour rechercher le mot entier.
   - **Couleur** : Cliquez sur ▾ et sélectionnez la couleur d'affichage des mots-clés trouvés.
9) Utilisez une des méthodes suivantes :
   - Cliquez sur **Appliquer** pour enregistrer la liste de surveillance et garder l'éditeur de liste de surveillance ouvert.
   - Cliquez sur **OK** pour enregistrer la liste de surveillance et fermer l'éditeur de liste de surveillance.
   - Cliquez sur **Annuler** pour fermer l'éditeur de liste de surveillance sans enregistrer vos modifications.



5.7.2. Modifier une liste de surveillance

1) Dans l'éditeur de liste de surveillance, sélectionnez la liste que vous souhaitez modifier.
2) Modifiez les paramètres et les mots-clés de la liste personnalisée, à votre convenance.
3) Pour filtrer la liste de mots-clés afin de localiser un mot-clé spécifique, saisissez celui-ci dans la case **Saisir le texte à filtrer**.
4) Pour modifier un mot-clé, cliquez sur celui-ci dans la liste, puis modifiez-le.
5) Pour supprimer un mot-clé, cliquez sur .
6) Lorsque vous avez terminé, procédez d'une des façons suivantes :
   - Cliquez sur **Appliquer** pour enregistrer la liste de surveillance et garder l'éditeur de liste de surveillance ouvert.
   - Cliquez sur **OK** pour enregistrer la liste de surveillance et fermer l'éditeur de liste de surveillance.
   - Cliquez sur **Annuler** pour fermer l'éditeur de liste de surveillance sans enregistrer vos modifications.

5.7.3. Importer une liste de surveillance

Les fonctions d'exportation et d'importation vous permettent de partager vos listes de surveillance et de recevoir celles de vos collègues. Importez des listes de surveillance existantes (fichiers *.csv) qui ont été enregistrées ou créées par UFED Logical Analyzer.

Vous pouvez également importer un fichier CSV qui contient une liste de mots clés, que vous pouvez ensuite utiliser comme mots clés de liste de surveillance. Cette option permet d'importer les mots clés sans formatage et recherche tous les types de données par défaut.

1) Dans la barre d'outils principale, cliquez sur .

   L'éditeur de liste de surveillance s'affiche.

2) Cliquez sur , et sélectionnez **Importer**.
3) Accédez à votre liste de surveillance, sélectionnez le fichier CSV, puis cliquez sur **Ouvrir**.



La liste de surveillance s'affiche dans l'éditeur de liste de surveillance. En voici un exemple :

Keywords   New   Enter text to filter ...

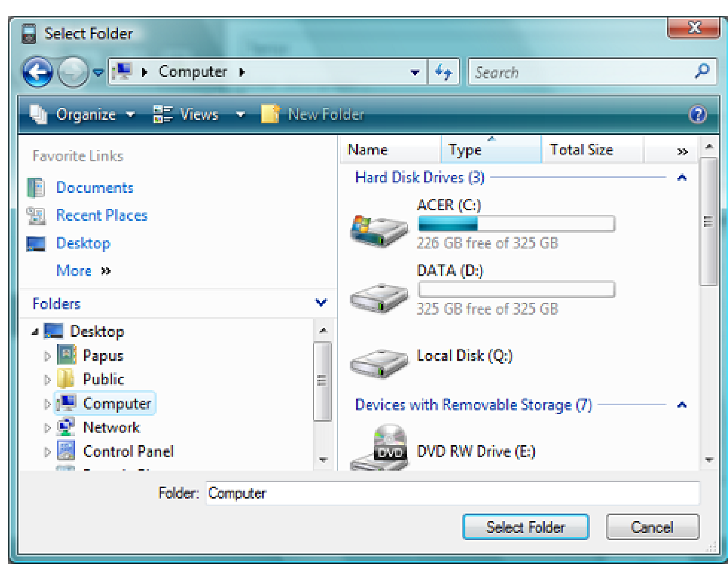
Entry Value	Match case	Whole word	Color	
ACID HEAD	☐	☑		
ANGEL DUST	☑	☐		
BAG	☐	☑		
BALLOON	☐	☑		
BRICK	☐	☑		
BROWNIES	☐	☐		
CANDY	☐	☐		
CANDYMAN	☐	☐		
COKE	☐	☐		
COOKER	☐	☐		
CUT	☐	☐		

5.7.4. Exporter une liste de surveillance

Exportez des listes de surveillance pour enregistrer une liste comme fichier *.csv, afin de la réutiliser ultérieurement ou de la partager avec d'autres personnes.

1) Dans l'éditeur de liste de surveillance, sélectionnez la liste que vous souhaitez exporter.

2) Cliquez sur .

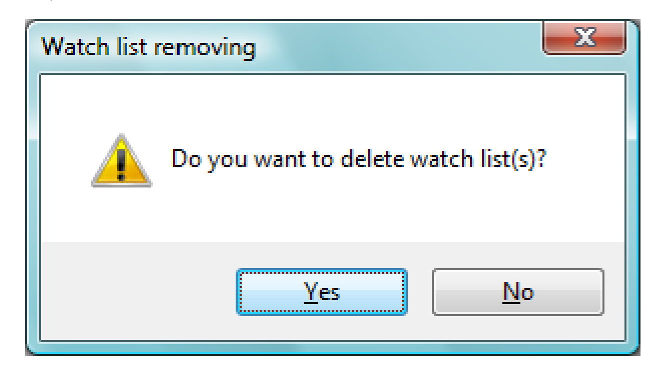




3) Accédez à l'emplacement dans lequel vous souhaitez enregistrer votre liste de surveillance, puis cliquez sur **Sélectionner dossier**.
4) La liste de surveillance est exportée. Par défaut, elle est enregistrée comme [nom de la liste de surveillance].csv.

5.7.5. Supprimer une liste de surveillance

1) Dans l'éditeur de liste de surveillance, sélectionnez la liste que vous souhaitez supprimer.
2) Cliquez sur ✖.



3) Cliquez sur **Oui**.

La liste de surveillance est supprimée.

5.7.6. Exécuter une liste de surveillance

Vous pouvez exécuter des listes de surveillance sur les projets ouverts.

5.7.6.1. Exécuter une liste de surveillance sur des projets spécifiques

Lorsque vous exécutez une liste de surveillance depuis l'éditeur de liste de surveillance, vous pouvez sélectionner les listes à exécuter et sur quels projets vous souhaitez les exécuter.

1) Dans la barre d'outils, cliquez sur pour ouvrir l'éditeur de liste de surveillance, puis sélectionnez la liste que vous souhaitez exécuter.
2) Cliquez sur .

   Une liste des projets ouverts s'affiche.
3) Sélectionnez le ou les projets ouverts sur lesquels vous souhaitez exécuter la recherche.

   REMARQUE : Une coche () indique que la liste de surveillance sélectionnée est active pour le projet.
4) Cliquez sur **Appliquer**.



UFED Logical Analyzer recherche les mots-clés dans les projets sélectionnés. Une fois la recherche terminée, les résultats de la liste de surveillance s'affichent dans l'élément d'arborescence **Listes de surveillance**.

Si la liste de surveillance est attribuée à des types d'informations spécifiques (voir ***Créer une liste de surveillance*** (page ***87***)), seules les correspondances pour ces types s'affichent dans les résultats.

5.7.6.2. Exécuter une liste de surveillance sur votre projet en cours

Lorsque vous exécutez une liste de surveillance depuis l'arborescence de projet, vous pouvez sélectionner quelles listes exécuter pour le projet sur lequel vous êtes en train de travailler. Si plusieurs projets sont ouverts, les listes de surveillance sélectionnées s'exécutent sur le dernier projet sur lequel vous avez cliqué dans l'arborescence de projet.

1) Dans la barre d'outils, cliquez sur .

   Une liste des listes de surveillance s'affiche.

2) Sélectionnez la ou les listes de surveillance que vous souhaitez exécuter sur le projet en cours.

   REMARQUE : Une coche () indique que la liste de surveillance est active pour le projet.

3) Cliquez sur **Appliquer** sur le projet mis en évidence dans l'arborescence de projet.

REMARQUE : Lorsque vous cliquez sur dans la barre d'outils, vous ne pouvez exécuter les listes de surveillance que sur le dernier projet sur lequel vous avez cliqué dans l'arborescence de projet.

UFED Logical Analyzer recherche les mots-clés dans les projets sélectionnés. Une fois la recherche terminée, les résultats de la liste de surveillance s'affichent dans l'élément d'arborescence **Listes de surveillance**.

Si la liste de surveillance est attribuée à des types d'informations spécifiques (voir ***Créer une liste de surveillance*** (page ***87***)), seules les correspondances pour ces types s'affichent dans les résultats.

5.8. Informations sur les signets (signets d'entités)

Un signet d'entité est un pointeur de référence rapide que vous pouvez créer pour des éléments individuels :

- Un élément de **Données analysées** tel qu'un appel du journal d'appels, un contact, un e-mail, etc. Consultez l'élément *Données analysées* dans la section ***Arborescence de projet*** (page ***46***).
- Un élément de **Fichiers de données** tel qu'un fichier image, un fichier vidéo, un fichier texte, etc. Consultez l'élément *Fichiers de données* dans la section ***Arborescence de projet*** (page ***46***).



Les signets d'entités que vous créez sont gérés dans l'élément **Signets d'entités** de l'arborescence. Le nombre de signets d'entités du projet apparaît entre parenthèses à côté du nom de la section.

- Double-cliquez sur **Signets d'entités** pour ouvrir une liste des signets d'entités dans un onglet dans la zone d'affichage des données. Les signets d'entité sélectionnés seront inclus dans les rapports générés.
- Double-cliquez sur un signet d'entité pour aller à l'élément marqué dans l'onglet d'affichage correspondant.

  Par exemple, double-cliquez sur un signet d'entité correspondant à un SMS pour ouvrir la liste de SMS dans un onglet d'affichage des Données analysées, avec l'élément marqué mis en surbrillance.
- Passez avec le curseur de la souris au-dessus d'un pour afficher le nom et la description du signet.
- Pour imprimer ou exporter uniquement la liste de signets d'entités, cliquez sur le format souhaité dans la barre d'outils de l'onglet **Signets d'entités** : Excel , HTML , PDF ou XML .

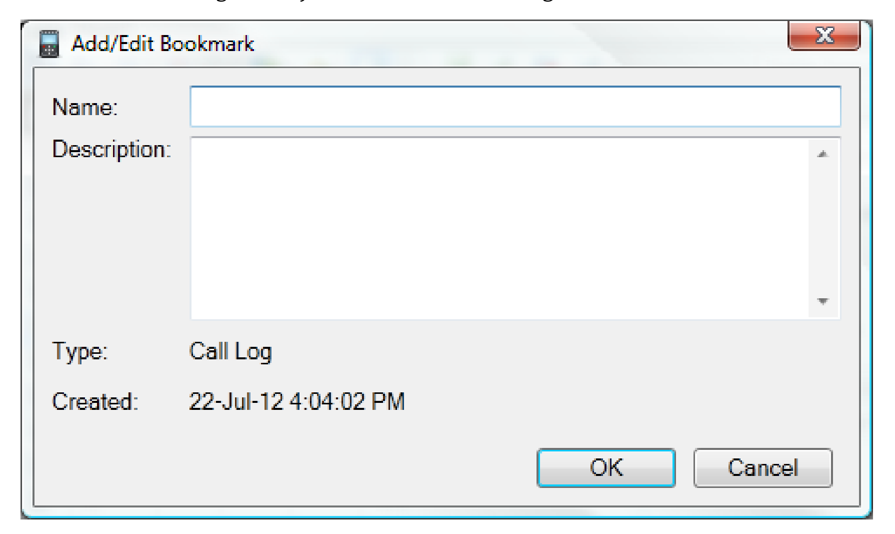
5.8.1. Créer un nouveau signet d'entité

Vous pouvez ajouter des signets d'entités aux éléments de la vue Tableau.

1) Sélectionnez l'élément auquel vous voulez ajouter un signet.

2) Cliquez sur .

La boîte de dialogue « Ajouter/modifier un signet » s'affiche.



3) Saisissez un nom et une description pour le nouveau signet d'entité, puis cliquez sur **OK**.

Un signet d'entité pointé vers l'élément sélectionné est ajouté à la liste de signets d'entités du projet. L'enregistrement d'élément marqué par un signet est indiqué par une bleue.



5.8.2. Modifier un signet d'entité

1) Choisissez une des options suivantes :

- Un enregistrement de signet d'entité dans la liste des **Signets d'entités** de l'arborescence du projet.
- Un élément marqué par un signet (indiqué par).

2) Cliquez sur dans la barre d'outils de la vue Tableau.

   La boîte de dialogue « Ajouter/modifier un signet » s'affiche.

3) Modifiez le nom ou la description, puis cliquez sur **OK**.

5.8.3. Supprimer un signet d'entité

1) Choisissez une des méthodes suivantes :

- Un enregistrement de signet d'entité dans la liste des **Signets d'entités** de l'arborescence du projet.
- Un élément marqué par un signet (indiqué par).

2) Cliquez sur dans la barre d'outils de la vue Tableau.

   Le signet est supprimé.

Chapitre 6 : **Traduction de données décodées**

Traduisez le contenu de vos extractions en langue étrangère sans attendre qu'un traducteur soit disponible, ni utiliser d'outils en ligne.

La fonction Traduction permet de traduire les données décodées sur demande, pour permettre aux enquêteurs de comprendre les informations disponibles dans une extraction. La fonction Traduction est une solution de traduction hors connexion, qui ne nécessite pas d'être connecté à Internet. Vous pouvez sélectionner une, plusieurs ou toutes les entrées du tableau pour les traduire. Le texte d'origine et le texte traduit peuvent être inclus dans le rapport.

Les langues prises en charge sont les suivantes :

Chinois (simplifié)	Japonais (payant)
Chinois (traditionnel)	Coréen
Néerlandais	Polonais
Allemand	Portugais
Hébreu	Russe
Italien	Espagnol
Français	Ukrainien



6.1. Utilisation de la fonction

Pour utiliser cette fonction, procédez de la façon suivante :

- Mettez à jour votre licence avec les langues de traduction sélectionnées.
- Téléchargez le package de traduction.
- Traduisez les données décodées.

6.2. Mettre à jour votre licence avec les langues sélectionnées

Vous pouvez sélectionner jusqu'à cinq langues gratuitement sur la page Mes produits dans MyCellebrite. Si vous avez besoin de langues supplémentaires, vous pouvez acheter le Pack Langue basique. Vous ne pouvez pas modifier une langue après l'avoir enregistrée, mais vous pouvez demander des langues supplémentaires.

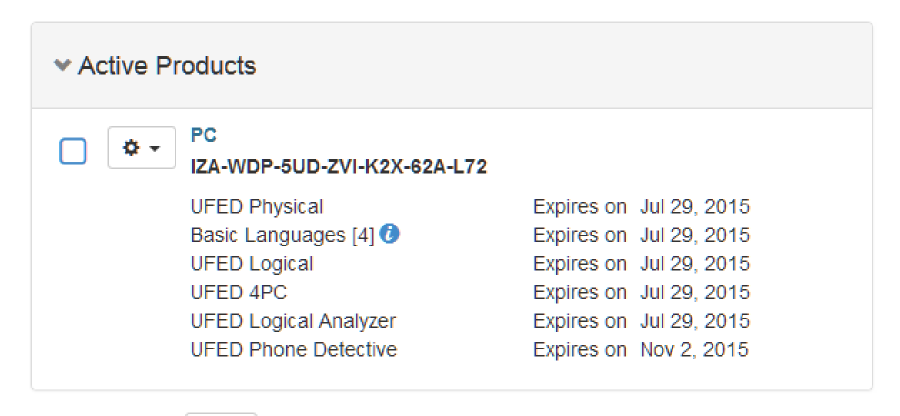
REMARQUE : Si vous souhaitez effectuer la traduction vers une langue autre que l'anglais, vous devez également la sélectionner.

Une fois votre licence produit mise à jour avec les langues sélectionnées, suivez la procédure ci-dessous pour consulter les langues incluses dans la licence de traduction.

6.2.1. Sélectionner des langues dans MyCellebrite

Pour sélectionner des langues :

1) Connectez-vous à MyCellebrite et sélectionnez l'onglet **Mes produits**. La fenêtre suivante s'affiche :



2) Sélectionnez , puis cliquez sur **Sélectionner les langues**. La fenêtre suivante s'affiche :



Device Languages for IZAWDP5UDZVIK2X62AL72 ×

Choose up to 5 languages for translating decoded data.

Tip: If you want to translate to a language other than English you should select it as well.

You cannot change a language after saving, but you don't have to choose all 5 right now.

Select Language ▲

Select Language ▲

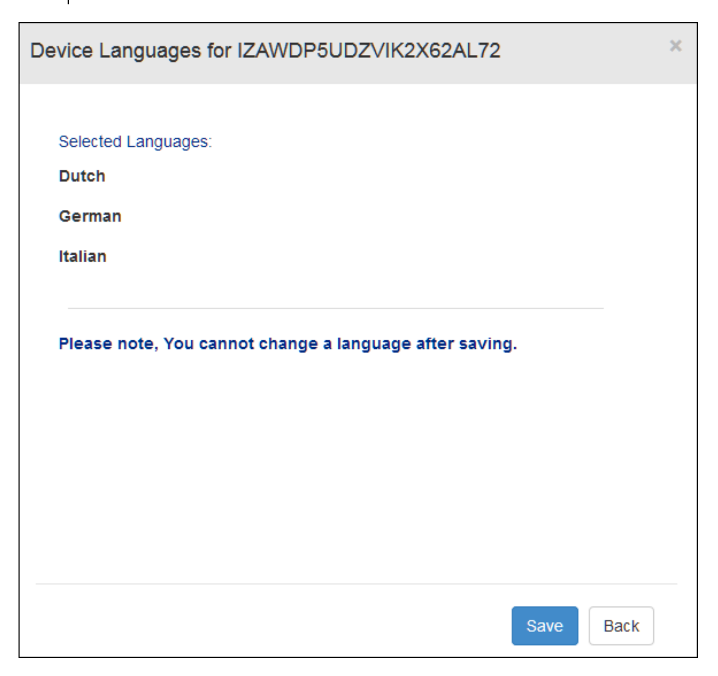
Select Language ▲

Select Language ▲

Select Language ▲

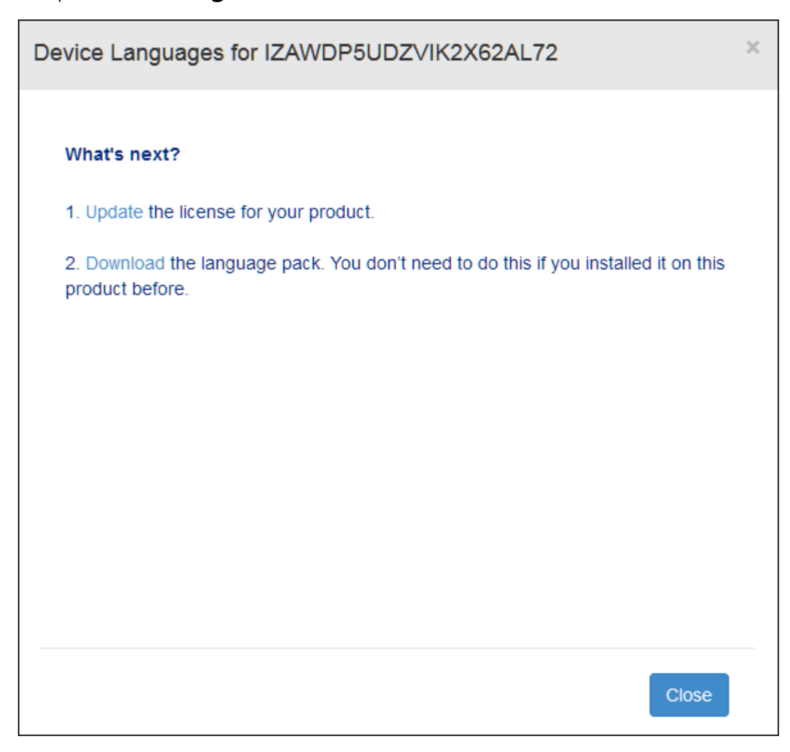
Need more languages? Next Cancel

3) Sélectionnez jusqu'à cinq langues de traduction, puis cliquez sur **Suivant**. La fenêtre suivante s'affiche : Pour des langues supplémentaires, cliquez sur **Besoin de langues supplémentaires** et remplissez le formulaire.





4) Cliquez sur **Enregistrer**. La fenêtre suivante s'affiche :



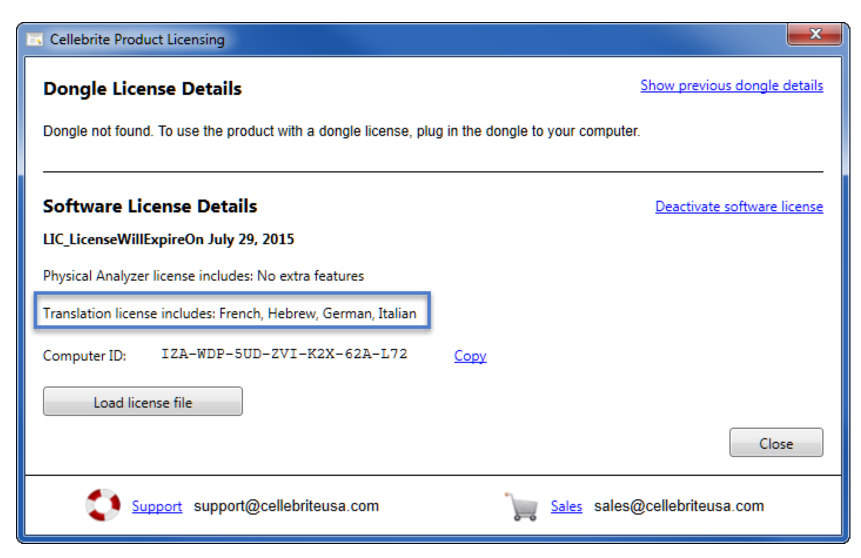
5) Mettez à jour la licence pour le produit, puis téléchargez le package de langues.

Une fois votre licence produit mise à jour avec les langues sélectionnées, suivez la procédure ci-dessous pour afficher les langues incluses dans la licence de traduction.

Pour consulter les langues de la licence de traduction :

- Sélectionnez **Outils** > **Traduction** > **Afficher les langues prises en charge**.

L'écran suivant s'affiche :





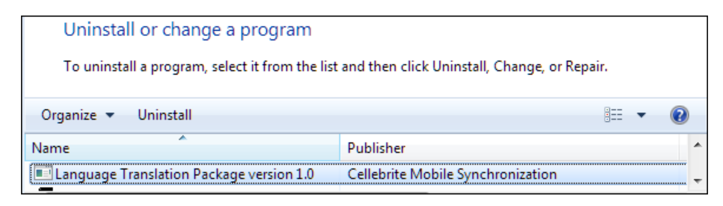
6.2.2. Télécharger le package de traduction

Vous pouvez télécharger le package de traduction depuis l'application ou depuis votre compte my.cellebrite.com. Le package de traduction inclut un numéro de version, qui vous permet de suivre la version installée sur l'ordinateur.

Pour télécharger le package de traduction :

1) Sélectionnez **Outils** > **Traduction.**
2) Choisissez l'une des options suivantes :
    - **Télécharger le package de traduction :** Télécharge le package de traduction (cette option n'est pas disponible si vous n'êtes pas connecté à Internet).
    - **Installer le package de traduction à partir d'un fichier :** Installe le package de traduction à partir d'un fichier. Sélectionnez cette option si vous n'êtes pas connecté à Internet.
3) Suivez les instructions à l'écran pour installer le package de traduction.

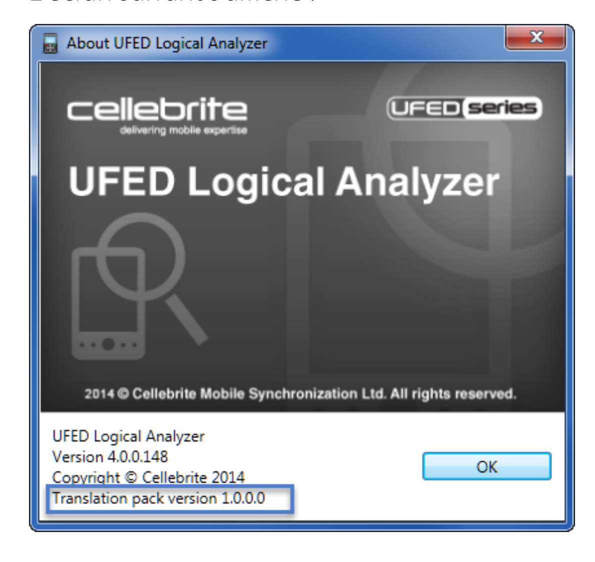
REMARQUE : Pour désinstaller le package de traduction, rendez-vous sur la page Désinstaller de Windows, et sélectionnez le package de traduction des langues (Publisher : Cellebrite Mobile Synchronization) dans la liste.



Pour afficher le numéro de version du package de traduction :

- Cliquez sur **Aide** > **À propos**.

  L'écran suivant s'affiche :





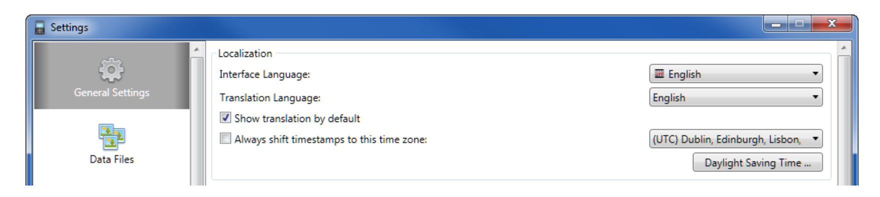
6.2.3. Traduction de données décodées

Par défaut, la langue cible définie est la même que la langue de l'interface. Si nécessaire, vous pouvez choisir une langue cible différente.

Pour modifier la langue de traduction :

1) Sélectionnez **Outils** > **Paramètres**.

   L'écran suivant s'affiche :

2) Sélectionnez la langue de traduction. C'est la langue dans laquelle vous souhaitez traduire le texte. Vous ne pouvez sélectionner qu'une seule langue cible. Pour demandez des langues de traduction supplémentaires, sélectionnez **Plus de langues**.

3) Cochez la case **Afficher la langue de traduction par défaut** pour afficher les traductions par défaut. Décochez cette case pour que la traduction n'apparaisse pas lorsque vous traduisez le texte. Pour afficher la traduction, sélectionnez **Afficher la traduction**.

Pour traduire des données décodées :

1) Cliquez sur les données que vous souhaitez traduire pour les sélectionner.

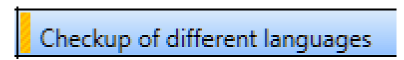
Überprüfung in verschiedenen Sprachen

2) Cliquez sur le bouton Translate ou sur le bouton droite de la souris et sélectionnez **Traduire la sélection**, ou cliquez sur , puis sélectionnez l'une des options suivantes :

- **Traduire tout :** Traduit toutes les entrées dans le champ spécifié.
- **Traduire la sélection :** Traduit uniquement le texte sélectionné.

REMARQUE : Si nécessaire, utilisez l'option **Supprimer la traduction** pour supprimer le texte traduit.

Le texte traduit est indiqué par une barre jaune.



Pour afficher le texte source :

3) Cliquez avec le bouton droit de la souris sur le texte et sélectionnez **Afficher la source**, ou cliquez sur le bouton View source.

Le texte source est indiqué par une barre grise.

Überprüfung in verschiedenen Sprachen



Pour filtrer le texte :

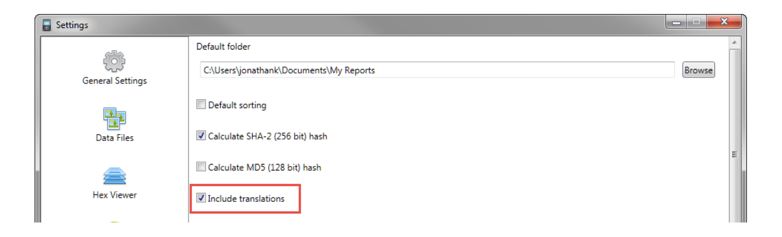
- Cliquez sur , puis sélectionnez l'une des options suivantes :
  - **Tout** pour afficher tout le texte.
  - **Traduit** pour afficher le texte traduit.
  - **Non traduit** pour afficher le texte non traduit.

6.2.4. Reporting

Lors de la création de rapports ou de l'exportation de données, vous pouvez préciser si vous souhaitez inclure le texte traduit ou non. Si vous choisissez d'afficher le texte traduit dans le rapport, le tableau de résumé inclut une entrée supplémentaire nommée : Langues traduites, avec une liste des langues. Le contenu traduit apparaît en-dessous du texte source, sous l'en-tête : Traduction. Pour plus d'informations sur les rapports, consultez la section ***Générer un rapport***, page ***131***.

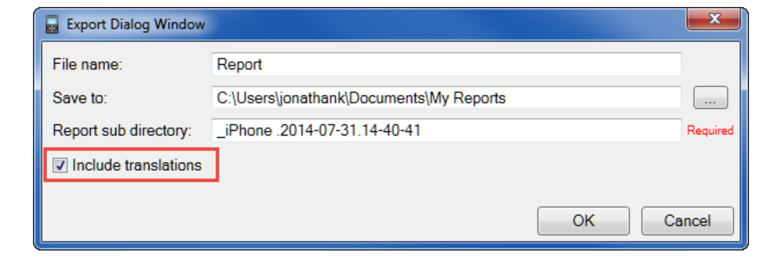
Pour inclure le texte traduit dans les rapports :

1) Allez dans **Outils** > **Paramètres** > **Paramètres généraux** > **Paramètres par défaut du rapport**.
2) Cochez la case **Inclure les traductions**.



Pour inclure le texte traduit dans les exportations :

1) Cliquez sur une option d'exportation ( ).
2) Cochez la case **Inclure les traductions**.




cellebrite
delivering mobile expertise

Chapitre 7 : **Travailler avec l'analyse de projet**

L'analyse de projet vous permet de visualiser les données de l'extraction en termes de nombre d'événements de communication entre l'appareil et d'autres parties, identifiées selon leur numéro de téléphone ou d'autres identifiants utilisateur (adresse e-mail, identifiant Skype, etc.). L'analyse vous permet d'identifier facilement et efficacement les schémas de communication entre l'appareil et les autres parties. Par exemple :

- Les parties avec lesquelles l'appareil communique le plus, via tous types de méthodes de communication ;
- Les parties avec lesquelles l'appareil communique le plus, via appels téléphoniques, SMS et MMS.

Si l'utilisateur de l'appareil a échangé un grand nombre d'appels téléphoniques, SMS et e-mails avec un certain contact, il est facile de voir le volume de ces communications. Les événements de communication sont répertoriés par volume et par type. Les événements de communication suivants sont pris en charge :

- **Téléphones** – répertorie les appels sortants, entrants et manqués, et les SMS et MMS envoyés et reçus, ainsi que les brouillons.
- **E-mails** – répertorie les e-mails envoyés, reçus, les brouillons et les e-mails de statut inconnu.



- **WhatsApp** – répertorie les messages envoyés, reçus et les brouillons.
- **Skype** – répertorie les appels, SMS et les messages instantanés.
- **BlackBerry Messenger** – répertorie les messages instantanés.

L'analyse du projet s'exécute automatiquement lorsque vous ouvrez un fichier d'extraction.

Pour afficher l'analyse de projet :

1) Cliquez sur ⊞ à côté de l'élément d'arborescence **Analyse du projet** pour afficher les résultats de l'analyse dans l'élément d'arborescence **Analyse du projet**.
2) Double-cliquez sur l'élément d'arborescence **Analyse du projet** pour ouvrir un onglet qui affiche les cinq activités les plus importantes par contact.
3) Pour afficher une vue d'ensemble comparative de tous les événements de communication, double-cliquez sur l'élément d'arborescence **Analyse de l'activité**.



La vue est triée par ordre croissant, en fonction du nombre total d'événements.



4) Pour afficher les événements par identifiant de communication, double-cliquez sur l'élément d'arborescence de l'identifiant souhaité.

5) Cliquez sur l'en-tête d'une colonne pour trier les informations dans celle-ci.

REMARQUE : Les informations de l'analyse de projet peuvent être incluses dans un rapport. Pour en savoir plus, consultez la section Générer un rapport.


cellebrite
delivering mobile expertise

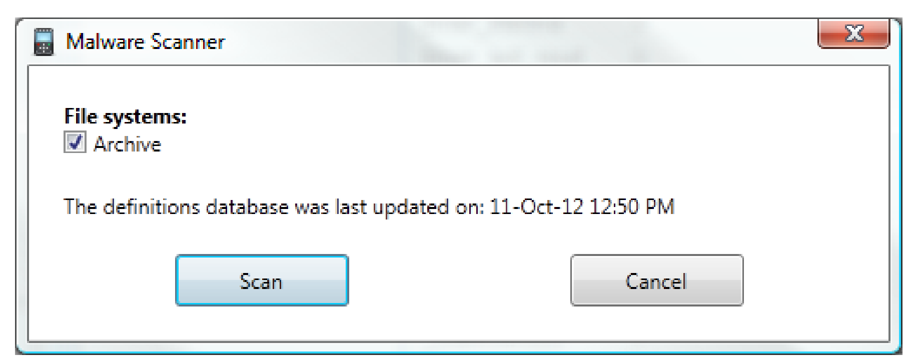
Chapitre 8 : **Rechercher les malware**

Exécutez la détection de malware sur votre extraction pour rechercher les malware.

Lors d'une recherche de malware, UFED Physical Analyzer utilise la dernière base de données de signature utilisée. Si vous utilisez le scanner anti-malware pour la première fois, ou si vous souhaitez mettre à jour la base de données avant d'effectuer le scan, suivez les étapes décrites dans la section ***Mettre à jour la base de données de signature (en ligne)*** (page ***123***). Si vous travaillez sur un ordinateur sans connexion Internet, suivez les étapes décrites dans la section ***Mettre à jour la base de données de signature depuis un fichier (hors connexion)*** (page ***124***).



1) Sélectionnez **Outils** > **Scanner anti-malware** > **Rechercher les malware** ou cliquez sur .



2) Sélectionnez le ou les systèmes que vous voulez scanner, puis cliquez sur **Scan**.

   UFED Physical Analyzer recherche les malware dans le projet. Les résultats sont affichés dans l'élément d'arborescence **Scanner anti-malware**.

3) Double-cliquez sur l'élément d'arborescence **Scanner anti-malware** pour ouvrir un onglet d'affichage des données.

   Les données affichées incluent le type de malware et les informations correspondantes, telles que le nom du malware.

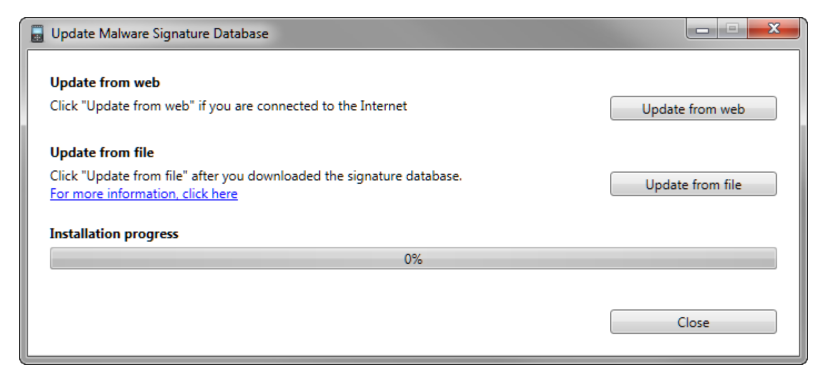
- Pour inclure les résultats dans un rapport, sélectionnez **Fichiers infectés** dans la zone **Ensemble de données du rapport**.

8.1. Mettre à jour la base de données de signature (en ligne)

Mettez à jour la base de données de signature avant d'utiliser le scanner anti-malware pour la première fois, afin de remplir la base de données, et ensuite afin de maintenir la base de données de signature à jour.

REMARQUE : Une fois la base de données de signature remplie, vous pouvez exécuter le scanner anti-malware en utilisant la base de données existante. Il est fortement conseillé de mettre à jour la base de données de signature régulièrement afin qu'elle reste à jour.

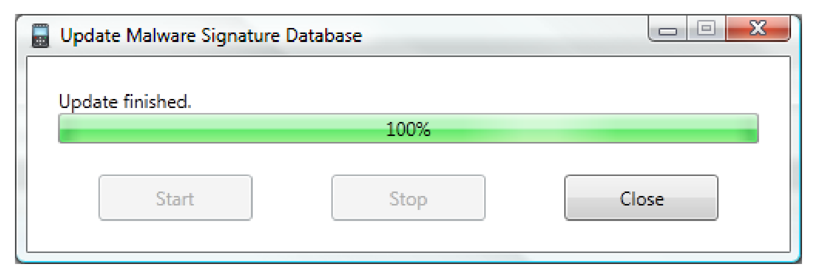
1) Dans le menu **Outils**, sélectionnez **Scanner anti-malware** > **Mettre à jour la base de données de signature**.



2) Cliquez sur **Mettre à jour depuis le serveur**.



La base de données est remplie.



3) Cliquez sur **Fermer**.

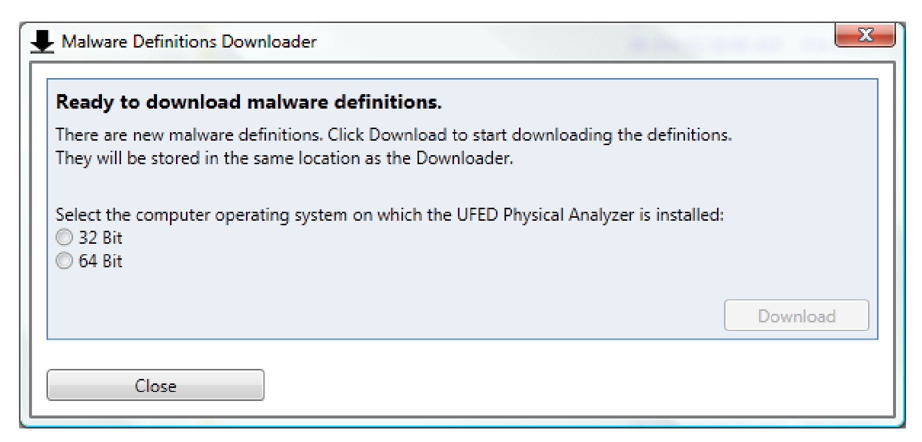
Vous pouvez maintenant scanner le projet pour rechercher des malware.

8.2. Mettre à jour la base de données de signature depuis un fichier (hors connexion)

Mettez à jour la base de données de signature à partir d'un fichier lorsque vous travaillez sur un ordinateur qui n'est pas connecté à Internet.

REMARQUE : Une fois la base de données de signature remplie, vous pouvez exécuter le scanner anti-malware en utilisant la base de données existante. Il est fortement conseillé de mettre à jour la base de données de signature régulièrement afin qu'elle reste à jour.

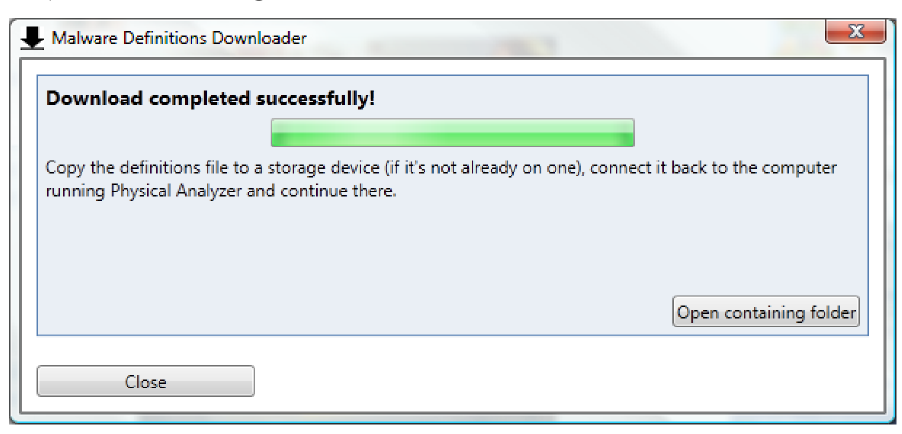
1) Dans Windows Explorer, dans le répertoire principal de UFED Physical Analyzer, copiez le répertoire **BitDefenderUpdater** sur un dispositif de stockage externe.
2) Transférez le répertoire **BitDefenderUpdater** sur un ordinateur connecté à Internet sans paramètres Proxy.
3) Dans le répertoire **BitDefenderUpdater**, double-cliquez sur **Malware Definitions Downloader.exe**.



4) Sélectionnez le système d'exploitation de l'ordinateur sur lequel UFED Physical Analyzer est installé.



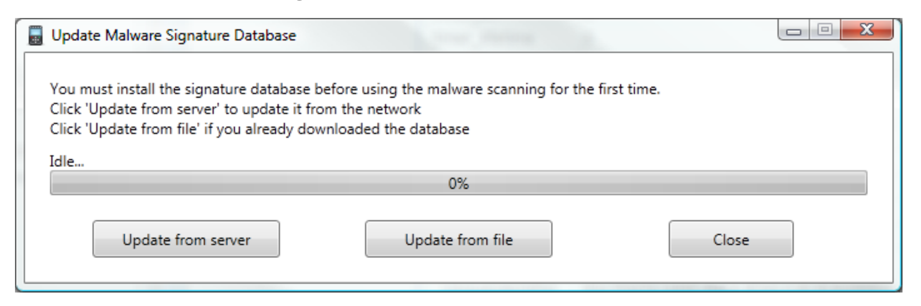
5) Cliquez sur **Télécharger**.



6) Cliquez sur **Ouvrir le dossier**.
7) Copiez le fichier **definitions.msd** sur un dispositif de stockage externe, puis transférez-le sur l'ordinateur sur lequel UFED Physical Analyzer est installé.
8) Cliquez sur **Fermer** pour fermer le programme de téléchargement des définitions de malware.

REMARQUE : Pour simplifier votre travail et gagner du temps, il est conseillé d'utiliser toujours le même ordinateur pour télécharger le fichier **definitions.msd**. Lorsque vous téléchargerez le fichier **definitions.msd** sur cet ordinateur à l'avenir, le programme de téléchargement des définitions de malware mettra à jour le fichier au lieu de le télécharger en totalité. Assurez-vous de ne pas supprimer le fichier **definitions.msd** de cet ordinateur.

9) Dans UFED Physical Analyzer, sélectionnez **Outils** > **Scanner anti-malware** > **Mettre à jour la base de données de signature**.



10) Cliquez sur **Mettre à jour depuis le fichier**.

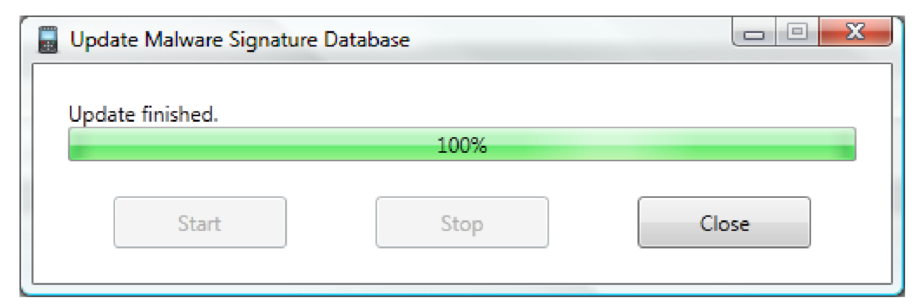


Open
« iPhone 4 (GSM) 4.3.2-4.3.3 File...
Search
Organize Views New Folder
Favorite Links
Documents
Recent Places
Desktop
More »
Folders
Desktop
Papus
Public
Computer
ACER (C:)
DATA (D:)
Name Date modified Type »
iPhone 4 (GSM) 4.3.2-4.3.3 File System ...
File name:
UFED dump (*.ufd)
Open Cancel

11) Accédez à au fichier de base de données de définitions des malware (*.msd), puis cliquez sur **Ouvrir**.

12) Cliquez sur **Démarrer**.

La base de données est remplie.



13) Cliquez sur **Fermer**.

Vous pouvez maintenant scanner le projet pour rechercher des malware.

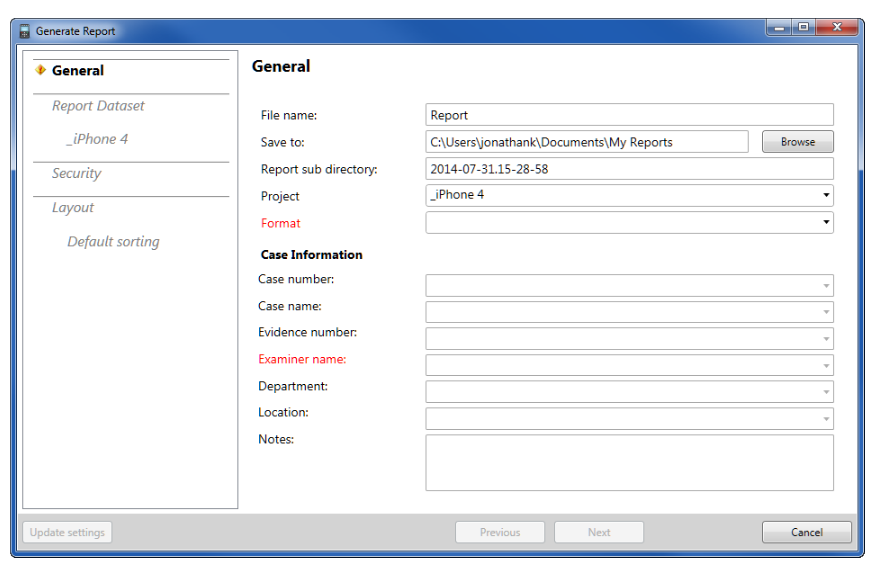

cellebrite
delivering mobile expertise

Chapitre 9 : **Générer un rapport**

1) Vous pouvez générer un rapport contenant les informations du projet. UFED Logical Analyzer fournit un assistant de création de rapport qui vous aide tout au long des étapes de la création d'un rapport. Utilisez une des méthodes suivantes :
   - Sélectionnez **Rapport** > **Générer un rapport** dans le menu de l'application.
   - Cliquez sur **Générer un rapport** dans l'onglet **Résumé d'extraction**.
   - Double-cliquez sur **Rapports** dans l'arborescence de projet.



L'écran Générer un rapport s'affiche.

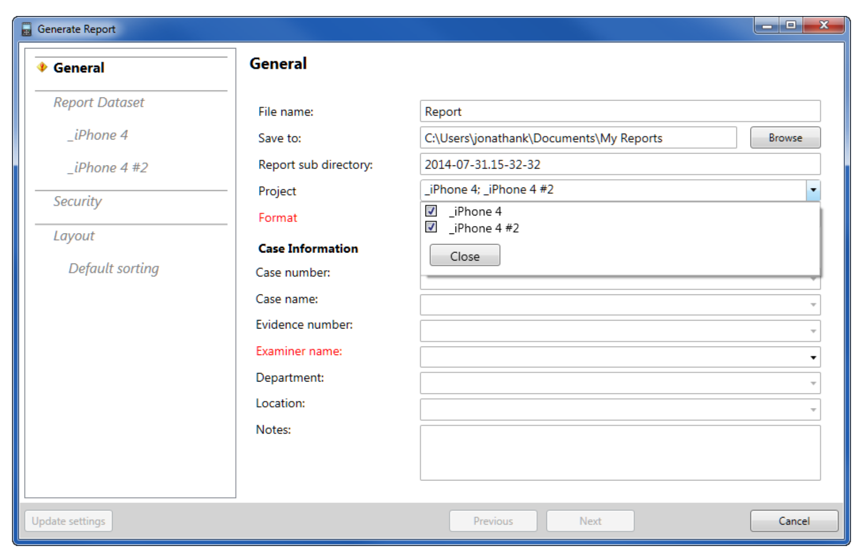


2) Dans **Nom de fichier**, sélectionnez le nom du nouveau rapport que vous souhaitez créer.

3) Dans **Enregistrer sur**, sélectionnez le dossier dans lequel vous souhaitez que tous les rapports soient créés. Ce dossier peut être utilisé pour tous les rapports, car chacun sera placé dans un sous-dossier distinct.

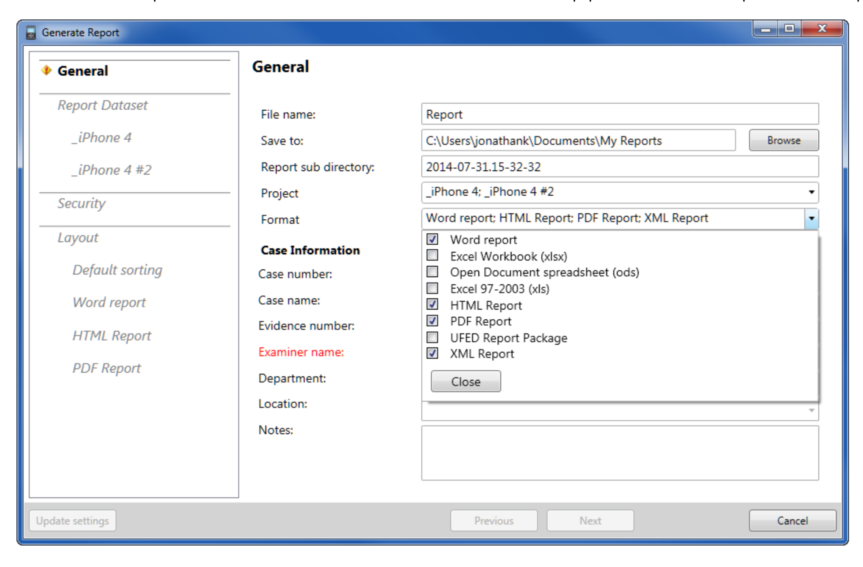
4) Dans **Sous-répertoire du rapport**, sélectionnez un nom pour le dossier dans lequel vous souhaitez que tous les rapports sélectionnez soient créés. Par défaut, ce nom est composé de la date et l'heure actuelles.

5) Dans **Projet**, sélectionnez le ou les projets que vous souhaitez inclure dans ce rapport. Seuls les projets déjà ouverts dans UFED Logical Analyzer peuvent être sélectionnés pour créer un rapport.





6) Dans le champ « Format », choisissez le format souhaité pour le rapport. Il est possible de sélectionner plusieurs formats. Dans ce cas, un rapport est créé pour chaque format.



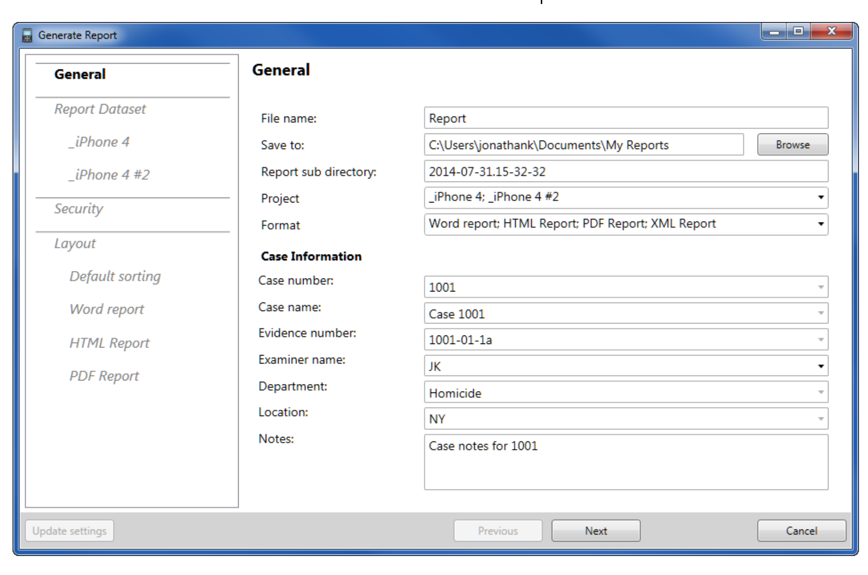
7) Pour les champs « Informations sur le cas », vous pouvez fournir les informations suivantes :

- **Numéro de cas**
- **Nom du cas**
- **Numéro de preuve**
- **Nom examinateur**
- **Service**
- **Lieu**

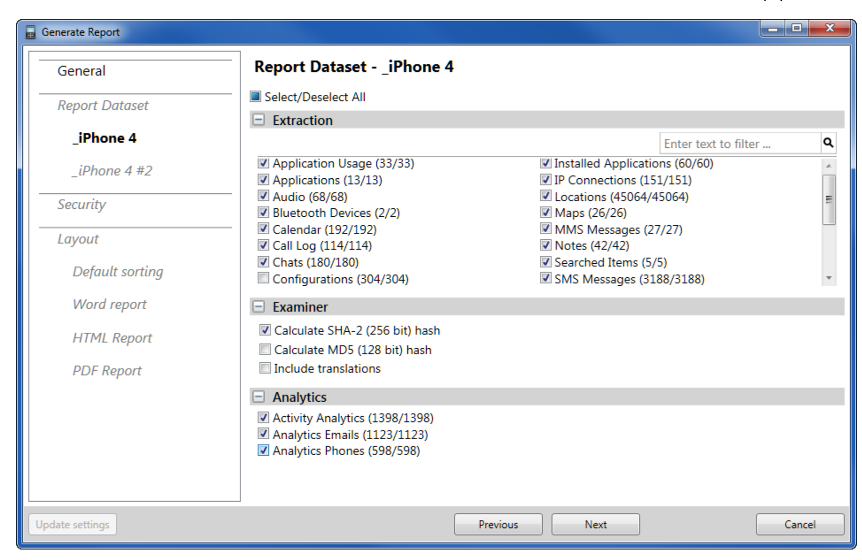
REMARQUE : Paramètres par défaut pour ces champs. Consultez la section ***Définir les informations du dossier*** (page ***189***). Consultez les sections ***Champs de rapport supplémentaires*** (page ***171***) et ***Paramètres par défaut du rapport*** (page ***175***) pour obtenir des paramètres par défaut supplémentaires. En outre, les 10 dernières valeurs saisies dans ces champs sont également disponibles dans la liste déroulante.



8) Votre formulaire doit alors ressembler à l'exemple ci-dessous :



9) Dans l'écran suivant, sélectionnez les données à inclure dans le rapport.



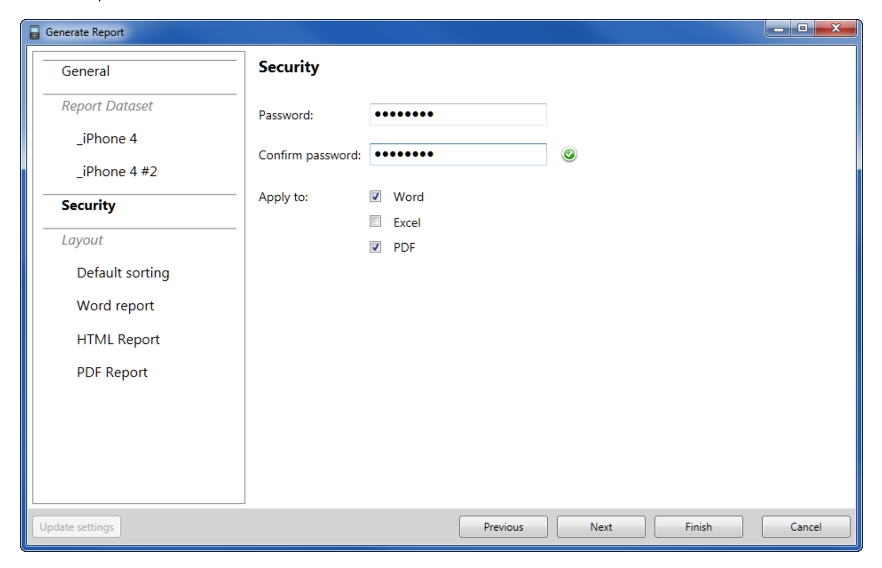
a) **Extraction** – données analysées et fichiers de données à inclure dans le rapport.



b) **Examinateur** – **Calculer le hachage SHA-2 (256 bits)** et **Calculer le hachage MD5 (128 bits)** – sélectionnez les clés de hachage MD5 et SHA256 calculées à ajouter à chaque élément des fichiers de données dans le rapport généré. Cette sélection concerne l'ensemble du rapport et s'applique à tous les projets contenus dans le rapport. CONSEIL : Pour raccourcir le processus de création de rapports pour les projets importants, ne sélectionnez pas ces options.

c) **Analyse** – cette section apparaît lorsque l'élément d'arborescence **Analyse** est disponible dans le projet. Sélectionnez les éléments d'analyse concernés pour les inclure dans le rapport.

10) L'écran **Sécurité** s'affiche. Les rapports au format PDF, WORD et Excel peuvent être protégés par mot de passe :

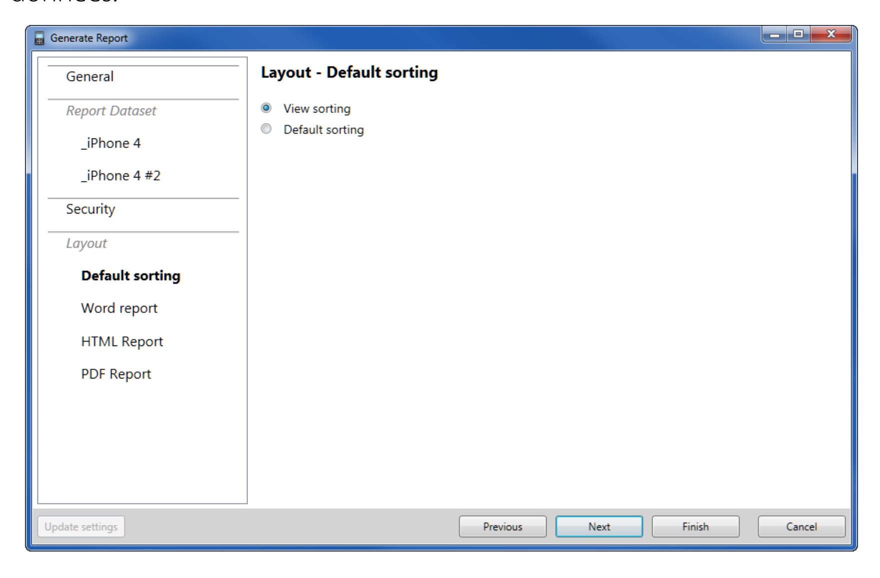


Choisissez le format et saisissez un mot de passe.

11) Sélectionnez **Tri par défaut** pour trier les éléments inclus dans le rapport généré en fonction du tri par défaut défini par Cellebrite pour chaque type de fichier analysé et de données, ou désélectionnez **Tri par défaut** pour trier les éléments en fonction du champ de tri sélectionné et



de l'ordre de tri (croissant ou décroissant) défini par l'utilisateur dans chaque tableau d'affichage de données.



12) Pour chaque format choisi pour ce rapport, vous pouvez préciser les paramètres de rapport de la façon suivante :

a) Rapports au format Word, HTML et PDF :

- **Désactiver la catégorisation des modèles** – sélectionnez cette option pour désactiver la séparation et générer un rapport dans lequel chaque élément de données est généré comme une section unique, sans séparation en sous-catégories. Par défaut, le rapport créé est organisé en catégories, et chaque catégorie du groupe d'éléments de données est générée comme section séparée du rapport. Par exemple, lorsque vous générez un rapport avec des SMS, cochez cette case pour générer les SMS sous forme de liste unique, ou décochez-la pour créer une liste distincte pour chaque catégorie de SMS (reçus, envoyés, brouillons, etc.).
- **En-tête du logo** – zone de texte dans laquelle vous pouvez saisir et personnaliser le format du texte qui s'affiche dans l'en-tête du rapport avant le logo.
- **Logo** – cliquez sur **Sélectionner un fichier image** pour ajouter l'image du logo à l'en-tête du rapport. Les formats compatibles sont : BMP, JPG, GIF et PNG.
- **Pied de page du logo** – saisissez et personnalisez le format du texte qui s'affiche dans le pied de page du rapport après le logo.
- **Afficher les totaux pour les éléments exclus du rapport** – ajoute une colonne **Total** au rapport qui affiche le nombre total d'éléments exclus du rapport.
- **Afficher le statut complet des éléments supprimés** – inclut le statut (**Intact**, **Supprimé** ou **Inconnu**) des éléments supprimés dans le rapport généré. Lorsque cette



option n'est pas sélectionnée, le statut des éléments supprimés est simplement « Oui », et reste vide pour les autres statuts.

- **Nombre de lignes de l'aperçu d'e-mail** – définit le nombre maximum de lignes affiché dans le rapport pour chaque e-mail.
- **Afficher le corps entier de l'e-mail** – affiche la totalité du corps du message.
- **Nombre de messages par chat** – définit le nombre maximum de messages affiché dans le rapport pour chaque conversation instantanée.
- **Afficher tous les messages des conversations instantanées** – affiche dans le rapport la totalité des messages des conversations instantanées.
- **Famille de police** – pour les rapports au format PDF uniquement.
- **Diviser le rapport HTML** – pour les rapports au format HTML uniquement. Garantit que chaque section du rapport commence sur une nouvelle page.

b) Rapports au format Excel (tous formats) et ODS :

- **Rapport Excel compatible avec OpenOffice** – sélectionnez cette option pour vous assurer que le rapport Excel pourra être ouvert sous OpenOffice.
- **Générer les données d'identification du contact** – sélectionnez cette option pour ajouter une feuille au rapport Excel contenant une liste des contacts uniques en fonction du type.

c) Package de rapport UFED et XML :

- AUCUN paramètre supplémentaire n'est requis pour ces rapports. Si les formats de rapport demandés incluent uniquement des rapports XML et/ou UFED, aucune information supplémentaire n'est nécessaire.

13) Cliquez sur **Terminer**.

REMARQUE : L'option **Terminer** ne devient disponible qu'une fois que les champs obligatoires sont remplis. Une icône d'avertissement jaune s'affiche à côté de tous les champs requis qui ne sont pas remplis.

Lorsque le rapport a bien été créé, vous êtes invité à ouvrir le fichier correspondant. Celui-ci s'ouvre avec l'application correspondant au format de fichier installée sur le poste de travail.

Une fois qu'un rapport été créé pour le projet, il est accessible dans la section Rapports de l'arborescence de projet. Double-cliquez sur le rapport de votre choix pour l'ouvrir avec l'application correspondante installée sur le poste de travail. Cliquez avec le bouton droit de la souris sur un rapport généré pour ouvrir le fichier du rapport, ou sélectionnez **Ouvrir le dossier** pour parcourir les fichiers et dossiers du rapport.


cellebrite
delivering mobile expertise

Chapitre 10 : **Effectuer des extractions**

10.1. Effectuer une extraction numérique avancée

Effectuez une extraction numérique avancée depuis UFED Logical Analyzer pour extraire davantage d'informations qu'avec l'extraction numérique à l'aide de l'unité UFED.

Vous pouvez effectuer une extraction numérique avancée depuis les appareils suivants :

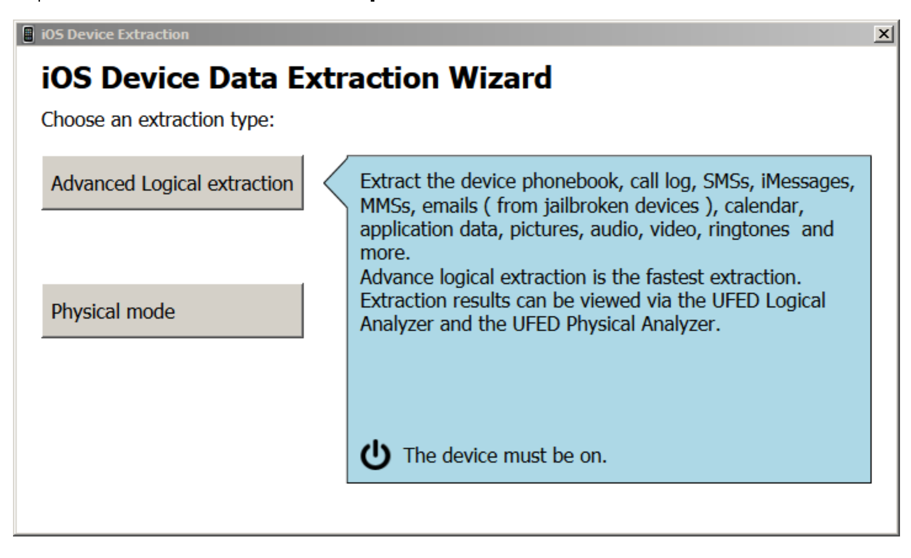
- iPhone 2G/3G/3GS/4/4s/5/5s/5c
- iPad 1/2/3/4/mini
- iPod Touch 1G/2G/3G/4G
- iPod Nano 5G



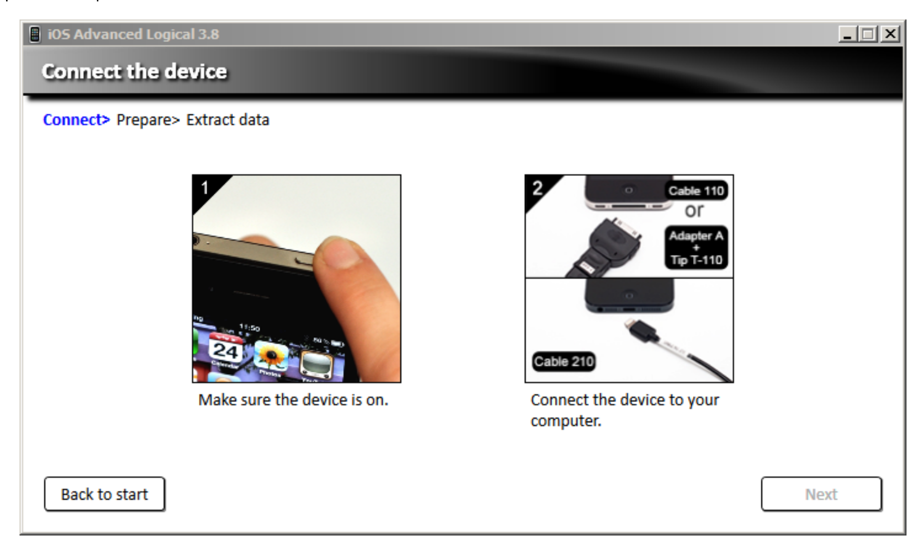
10.1.1. Effectuer une extraction numérique avancée

1) Sélectionnez **Extraire > Extraction d'appareils iOS** ou cliquez sur pour lancer l'extraction d'appareil iOS.

2) Cliquez sur **Extraction numérique avancée**.



3) Suivez les instructions qui s'affichent pour allumer l'appareil iOS et le connecter à votre ordinateur, puis cliquez sur **Suivant**.

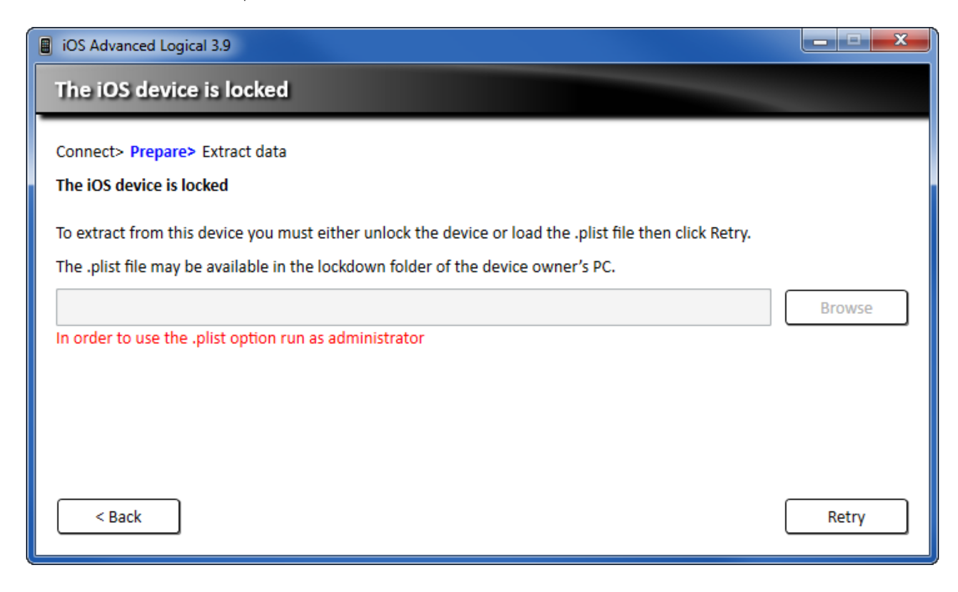


REMARQUE : Si l'appareil connecté n'est pas reconnu, déconnectez-le, puis reconnectez-le à un port USB à l'arrière de l'ordinateur.



Si l'appareil iOS est verrouillé, l'écran **Appareil verrouillé** s'affiche. Si le fichier .plist pour l'appareil verrouillé est disponible sur le PC du propriétaire de l'appareil, alors ce fichier .plist peut être chargé sur l'écran **Appareil verrouillé**. Cliquez ensuite sur **Réessayer**. Si l'appareil est verrouillé et qu'aucun fichier .plist n'est disponible, cliquez sur **Fermer**.

REMARQUE : Pour utiliser le fichier .plist, vous devez exécuter l'application UFED en tant qu'administrateur.



4) Choisissez une **Méthode** d'extraction numérique avancée. Selon que l'appareil est **bloqué** et/ou **crypté** ou non, différentes méthodes d'extraction sont disponibles :

   a) Méthode 1 – Extraction d'un ensemble de données important comprenant les SMS, MMS, données d'application et emplacements. Journaux des appels, corps des e-mails et pièces jointes ne sont pas extraits. Durée d'extraction prolongée.

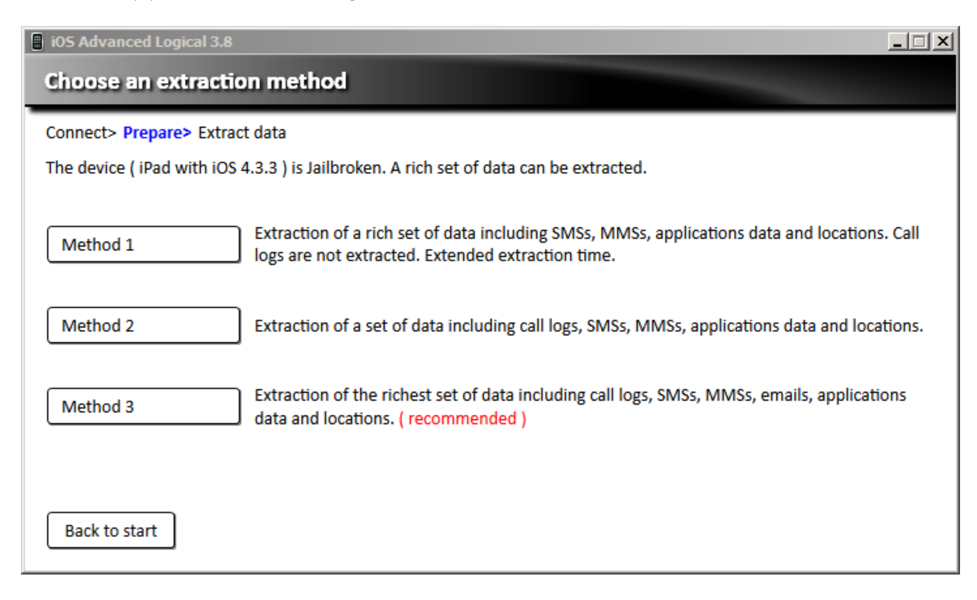
   b) Méthode 2 – Extraction d'un ensemble de données comprenant les journaux d'appels, SMS, MMS, données d'application et emplacements. Cette procédure de décodage peut nécessiter la saisie du mot de passe de sauvegarde iTunes.

   c) Méthode 3 – Extraction de l'ensemble de données le plus complet comprenant les journaux d'appels, SMS, MMS, e-mails, données d'application et emplacements.

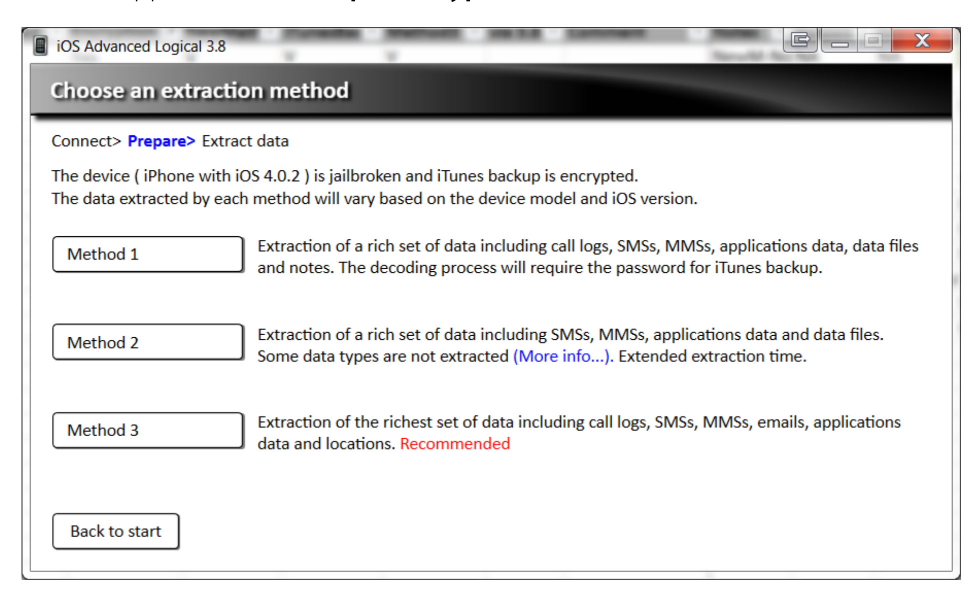
En outre, l'application indique une méthode recommandée spécifique en fonction de la configuration de la sauvegarde iTunes et de si l'appareil est bloqué ou non.



Pour un appareil iOS **débloqué**, l'écran suivant s'affiche :

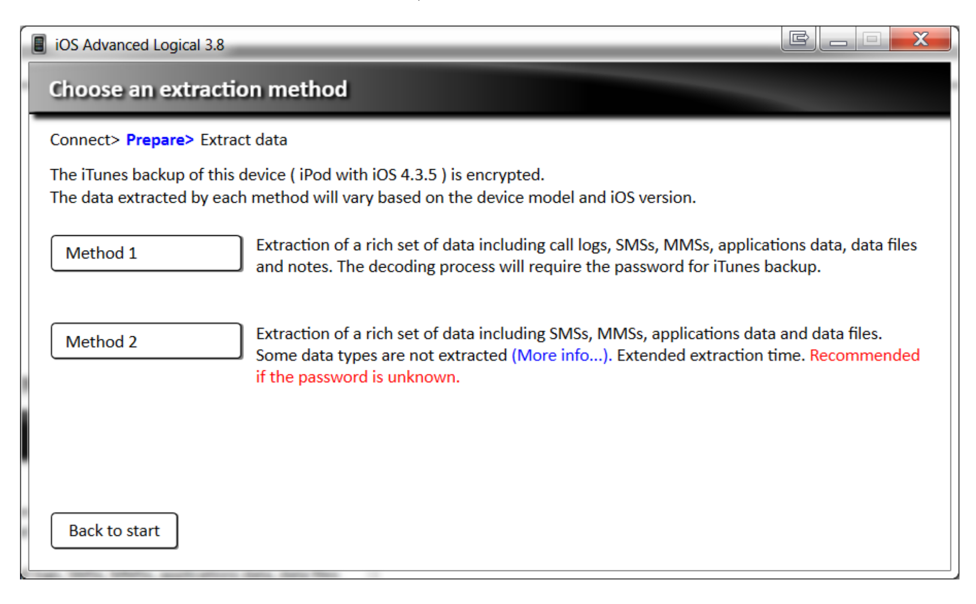


Pour un appareil iOS **débloqué et crypté**, l'écran suivant s'affiche :

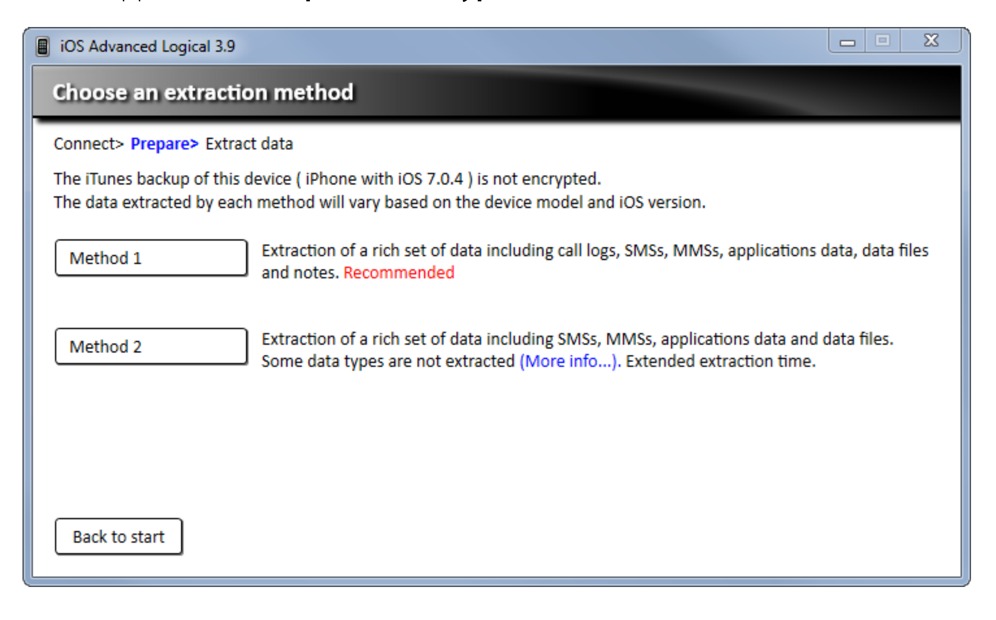




Pour un appareil iOS **bloqué et crypté**, l'écran suivant s'affiche :



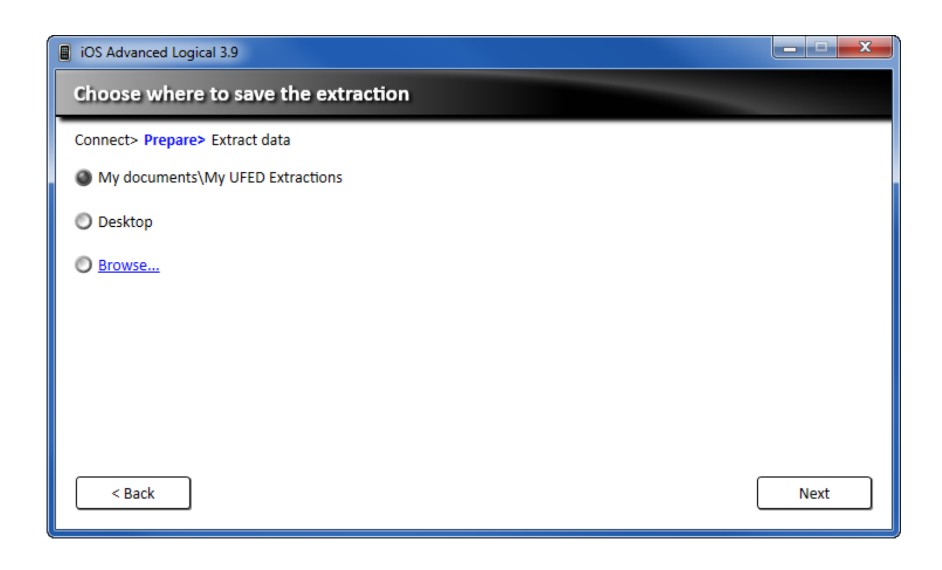
Pour un appareil iOS **bloqué et non crypté**, l'écran suivant s'affiche :





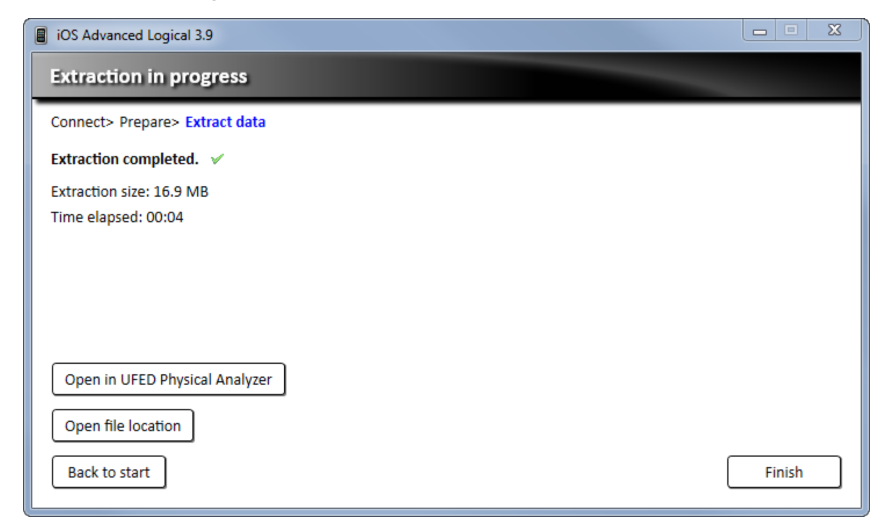
REMARQUE : La durée de l'extraction dépend de la quantité de données présente sur l'appareil iOS et de la méthode choisie. Une extraction avec la **Méthode 2** effectuée sur un appareil beaucoup utilisé peut durer plusieurs HEURES.

5) Choisissez l'emplacement où vous souhaitez enregistrer les données extraites. Assurez-vous que l'espace disque disponible est suffisant à l'emplacement choisi. Vous pouvez enregistrer les données localement sur l'ordinateur, sur un dispositif de stockage amovible ou sur le réseau.



6) Cliquez sur **Suivant** pour continuer.

7) Une barre de progression s'affiche. Attendez la fin du processus d'extraction.



REMARQUE : Sa durée varie en fonction de la méthode d'extraction, du modèle de l'appareil, de la quantité de données sur l'appareil, de l'ordinateur qui effectue l'extraction et d'autres paramètres.

L'extraction numérique avancée est enregistrée à l'emplacement choisi, sous la forme d'un fichier *.UFD et d'un fichier *.TAR.



Ouvrez l'extraction numérique avancée dans UFED Logical Analyzer pour accéder à toutes les informations extraites.

8) Choisissez l'une des options suivantes :

- **Ouvrir dans UFED Logical Analyzer** – charge le fichier d'extraction dans UFED Logical Analyzer.
- **Ouvrir l'emplacement du fichier** – ouvre le dossier qui contient les fichiers d'extraction.
- **Revenir au début** – revient à l'écran des méthodes d'extraction.
- **Terminer** – ferme l'extraction d'appareil iOS.

Chapitre 11 : **Preuve appareil photo et capture d'écran**

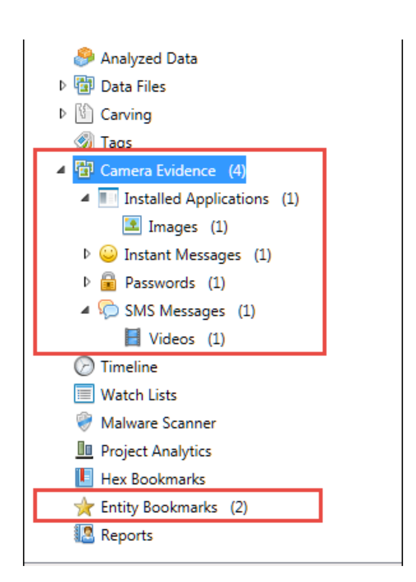
UFED 4PC ou UFED Touch associé à l'appareil photo UFED vous permet de rassembler des preuves en prenant des photos ou des vidéos d'un appareil. Une fonction Captures d'écran permet d'effectuer des captures d'écran en interne directement à partir d'un appareil Blackberry, Android ou iOS. Ces options peuvent être utiles pour réunir des preuves complémentaires, ou lorsqu'il est impossible d'extraire les données d'un appareil. Ces preuves peuvent être affichées dans UFED Logical Analyzer ainsi que des notes, catégories et signets ajoutés par l'examinateur. Pour plus d'informations sur la capture de preuves appareil photo et captures d'écran, reportez-vous aux manuels de l'utilisateur *UFED 4PC* ou *UFED Touch*.

Pour importer des preuves appareil photo ou capture d'écran :

- Cliquez sur le fichier Evidence.ufd.

  Les preuves appareil photo (images et vidéos) ou les preuves téléphone (captures d'écran) sont importées dans UFED Logical Analyzer comme nouveau projet. Les preuves incluent les preuves téléphone ou les preuves appareil photo, séparées en catégories, ainsi que les signets d'entité et notes ajoutés au cours de l'extraction. En voici un exemple :

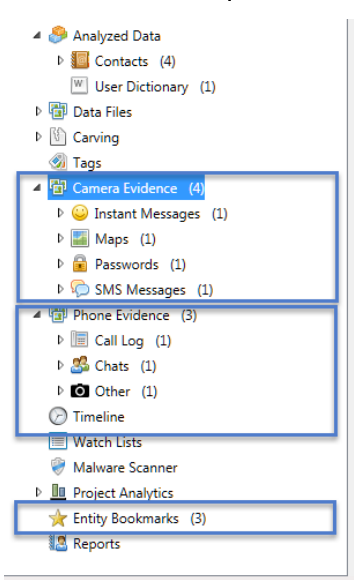

cellebrite
delivering mobile expertise


Analyzed Data
Data Files
Carving
Tags
Camera Evidence (4)
Installed Applications (1)
Images (1)
Instant Messages (1)
Passwords (1)
SMS Messages (1)
Videos (1)
Timeline
Watch Lists
Malware Scanner
Project Analytics
Hex Bookmarks
Entity Bookmarks (2)
Reports

Pour importer des preuves appareil photo et capture d'écran avec les données extraites :

- Cliquez sur le fichier EvidenceCollection.ufdx.

  Les preuves appareil photo (images et vidéos), les preuves téléphone (captures d'écran) et les données extraites sont importées dans UFED Logical Analyzer comme projet unique. Les preuves incluent les preuves téléphone ou les preuves appareil photo, ainsi que les catégories, signets d'entité et notes ajoutés au cours de l'extraction. En voici un exemple :



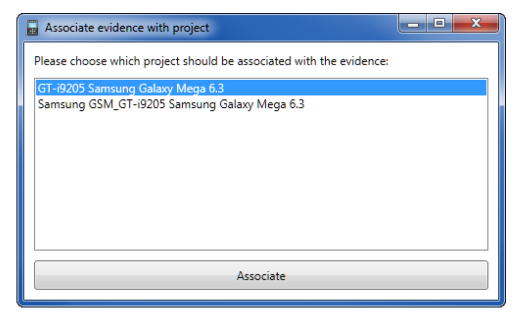


REMARQUE : Glissez-déposez le fichier EvidenceCollection.ufdx dans UFED Logical Analyzer pour ouvrir plusieurs extractions effectuées pour un appareil particulier. C'est-à-dire que toutes les extractions dans le dossier seront ouvertes. Chaque extraction (fichier .ufd) dans le dossier peut aussi être ouverte séparément. Un exemple de dossier avec plusieurs extractions et un fichier UFDX s'affiche ensuite.



Pour associer des preuves appareil photo et capture d'écran à un type d'extraction :

Si vous disposez de plusieurs types d'extraction ainsi que de preuves appareil photo, l'écran « Associer les preuves au projet » s'affiche.



- Sélectionnez l'extraction requise et cliquez sur **Associer**.

Chapitre 12 : **Paramètres**

La fenêtre « Paramètres » permet d'accéder aux options de configuration fonctionnelles et comportementales utilisées pour ajuster et contrôler les fonctionnalités et l'utilisation de l'application. Les paramètres de la fenêtre « Paramètres » s'appliquent à tous les projets ouverts dans UFED Logical Analyzer.

REMARQUE : Les modifications des paramètres sont perdues lorsque vous fermez UFED Logical Analyzer. Pour enregistrer la configuration des paramètres, consultez la section ***Enregistrer les paramètres*** (page ***184***).

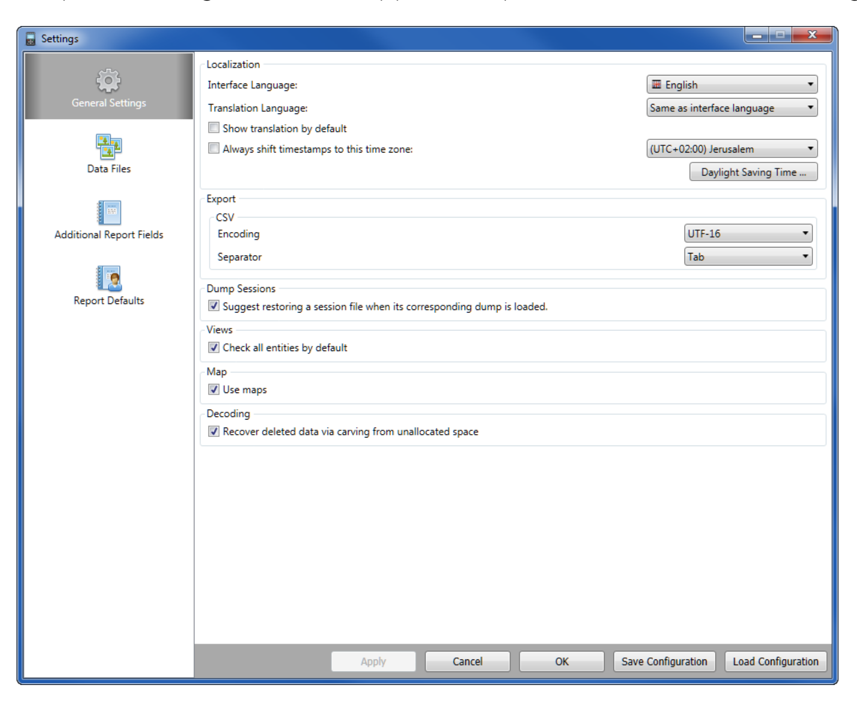
- Pour accéder à la fenêtre « Paramètres », procédez de l'une des façons suivantes :
  - Sélectionnez **Outils** > **Paramètres**.
  - Cliquez sur .

La fenêtre « Paramètres » s'affiche.



12.1. Paramètres généraux

Les paramètres généraux de l'application peuvent être définis dans l'onglet **Paramètres généraux**.



Pour configurer la langue de l'interface de UFED Logical Analyzer :

- Dans la liste **Langue**, sélectionnez la langue souhaitée.

Pour définir la langue de traduction :

- Sélectionnez la langue de traduction. C'est la langue dans laquelle vous souhaitez traduire le texte. Vous ne pouvez sélectionner qu'une seule langue de traduction. Pour demandez des langues de traduction supplémentaires, sélectionnez **Plus de langues**.
- Cochez la case **Afficher la langue de traduction par défaut** pour afficher les traductions par défaut. Décochez cette case pour que la traduction n'apparaisse pas lorsque vous traduisez le texte. Pour afficher la traduction, sélectionnez **Afficher la traduction**.

Pour déplacer les horodateurs vers un fuseau horaire particulier :

1) Dans la liste Paramètres de fuseau horaire (UTC), sélectionnez :
    - Valeur UTC originale pour afficher les horodateurs tels qu'ils ont été enregistrés (sans unification).
    - Un des fuseaux horaires (UTC -12:00 à UTC +13:00) pour recalculer les horodateurs définis par le réseau en fonction du décalage du fuseau horaire.
2) Pour modifier les dates de début et de fin de l'heure d'été, cliquez sur **Heure d'été**. Pour en savoir plus sur comment modifier les paramètres de fuseau horaire, reportez-vous à la section ***Définir un fuseau horaire unifié pour le projet*** (page *185*).



Pour configurer l'encodage et le séparateur des fichiers CSV exportés :

1) Dans la zone **Exporter**, sélectionnez l'option d'encodage souhaitée dans la liste **Encodage**.
2) Sélectionnez le séparateur souhaité dans la liste **Séparateur**.

Pour que UFED Logical Analyzer vérifie automatiquement les images au chargement du projet :

- Sélectionnez **Vérifier automatiquement les images au chargement du projet**.

Pour que UFED Logical Analyzer propose de charger une session à l'ouverture de l'extraction correspondante :

- Sélectionnez **Suggérer la restauration d'un fichier de session à l'ouverture du fichier de vidage correspondant**.

Pour sélectionner toutes les entités dans toutes les vues par défaut :

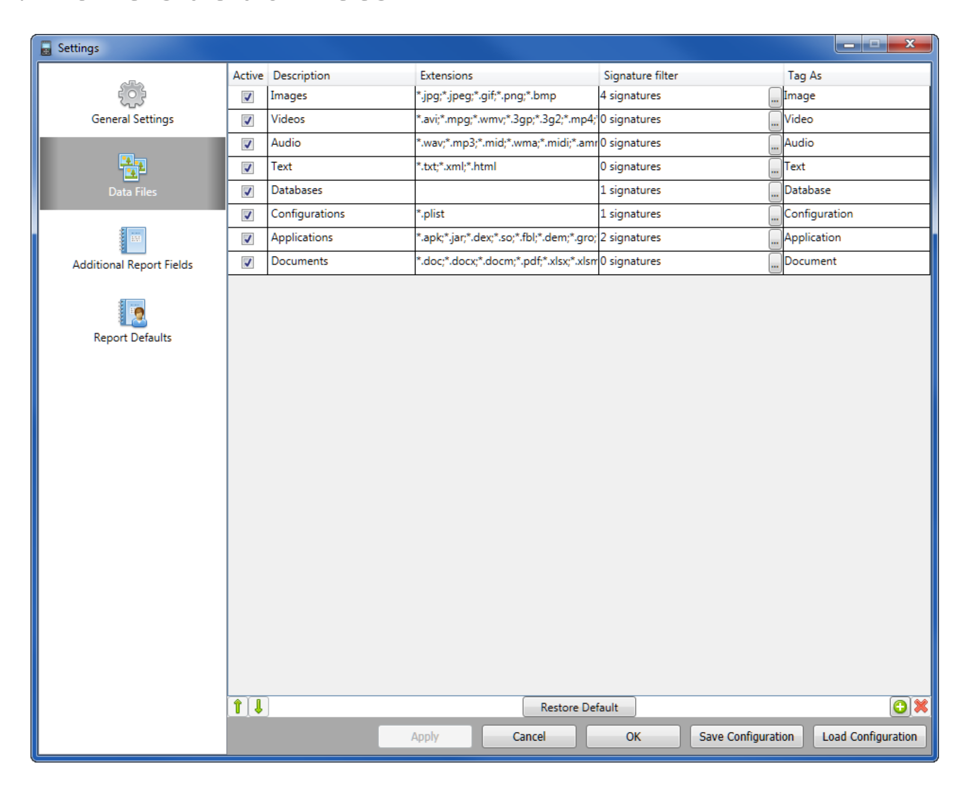
- Sélectionnez **Cocher toutes les entités par défaut**.

  Les entités sélectionnées seront incluses dans les rapports générés.

Pour déterminer le nombre de chiffres requis pour qu'un numéro de téléphone soit unique :

- Dans la zone **Analyse**, sélectionnez le nombre de chiffres souhaités dans le champ **Nombre de chiffres pour qu'un numéro de téléphone soit unique**.

12.2. Fichiers de données





Les paramètres des **Fichiers de données** déterminent les différents groupes de fichiers et de balises dans les éléments d'arborescence **Fichiers de données** et **Balises**, et les types de fichiers filtrés dans chaque groupe.

Chaque enregistrement de fichier de données contient les paramètres suivants :

- **Actif** – indique si le groupe de fichiers de données doit être affiché (coché) ou masqué (décoché) dans l'arborescence de projet.
- **Description** – nom descriptif pour le type de fichiers de données, utilisé comme nom de groupe dans l'élément d'arborescence **Fichiers de données**.
- **Extensions** – extensions de fichier à utiliser pour filtrer les fichiers de données de ce groupe.
- **Filtre signature** – signatures d'en-tête et/ou de pied de page à utiliser pour filtrer les fichiers de données de ce groupe.
- **Baliser comme** – nom de balise à appliquer au fichier de données et utilisé pour répertorier les fichiers dans l'arborescence de projet **Balises**.

12.2.1. Méthodes de filtrage des fichiers de données

Vous pouvez filtrer les groupes en utilisant une ou plusieurs des méthodes suivantes :

- Filtre signature

  Un filtre signature est une définition de l'en-tête et/ou du pied de page du fichier à rechercher, permettant de détecter un type de fichier et de l'associer à un groupe de fichiers de données spécifique. L'en-tête et/ou le pied de page peuvent être configurés sur une plage définie à partir du début et de la fin du fichier, respectivement, en utilisant le paramètre de décalage.

  Par exemple, une image au format JPEG commence par l'en-tête FF D8 FF et se termine par le pied de page FF D9. En saisissant ces informations dans les champs En-tête et Pied de page de la signature, vous créez une signature qui identifie les images au format JPEG.

- Filtre d'extension

  Un filtre d'extension est une liste d'extensions de fichier courantes associées aux formats de fichiers qui appartiennent au groupe de fichiers de données spécifique.

  Par exemple, il est possible de filtrer les différents formats des fichiers images par les extensions *.jpg, *.jpeg, *.gif, *.png ou *.bmp.



12.2.2. Gérer les paramètres des fichiers de données

Ajoutez de nouveaux types de fichiers de données, et modifiez et supprimez les types de fichiers de données existants.

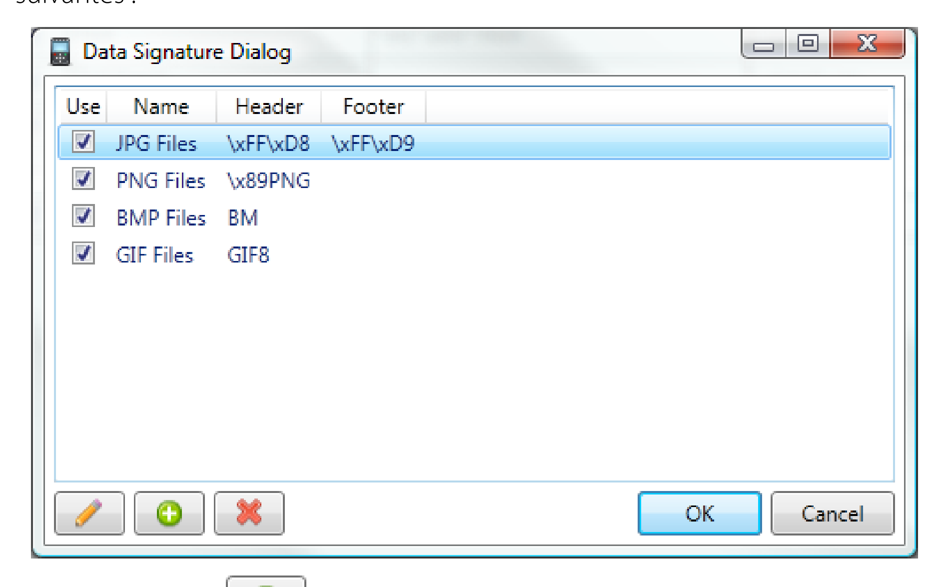
12.2.2.1. Ajouter un type de fichiers de données

1) Dans les paramètres **Fichiers de données**, cliquez sur .

   Une nouvelle ligne est ajoutée à la liste.

2) Sélectionnez **Actif** pour afficher le type de données ajouté dans l'élément d'arborescence **Type de données**.
3) Cliquez sur la fenêtre **Description** de la nouvelle ligne, et saisissez une description pour le type de fichiers.
4) Le cas échéant, dans la fenêtre **Extensions**, saisissez les extensions de fichier couramment utilisées par votre type de fichier de données au format ***.xxx**, et séparées par des points-virgules « **;** ».

5) Le cas échéant, dans la fenêtre **Filtre signature**, cliquez sur et choisissez une des options suivantes :



- Cliquez sur pour ajouter filtre signature qui identifie votre type de fichiers de données.
- Cliquez sur pour modifier un filtre signature existant.



- Cliquez sur pour supprimer un filtre signature.

6) Le cas échéant, dans la fenêtre **Baliser comme**, cliquez sur un nom de balise dans la liste pour le sélectionner.
7) Pour modifier l'ordre des types de fichiers de données, utilisez les flèches .
8) Pour effacer la liste de types de fichiers de données que vous avez ajoutés et conserver uniquement les types par défaut, cliquez sur **Rétablir la liste par défaut**.

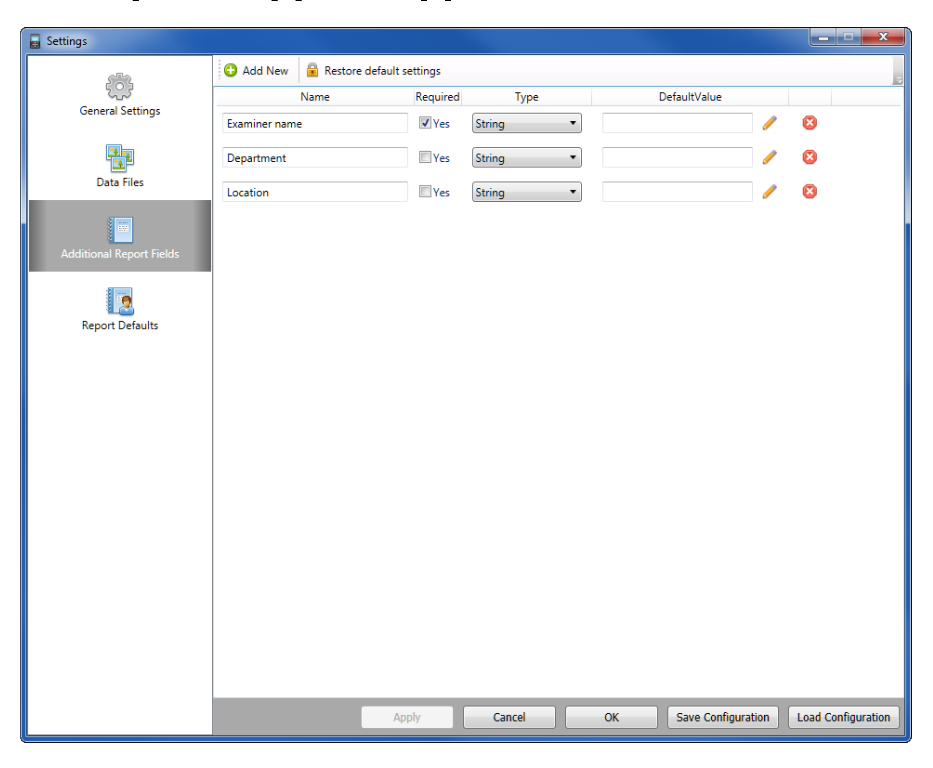
12.2.2.2. Modifier un enregistrement de fichier de données existant

1) Cliquez sur la ligne du type de fichiers de données que vous souhaitez modifier.
2) Double-cliquez sur la colonne et la ligne que vous souhaitez modifier, et mettez à jour les paramètres existants à votre convenance.

12.2.2.3. Supprimer un type de fichier de données

1) Cliquez sur la ligne du type de fichiers de données que vous souhaitez supprimer.
2) Cliquez sur .

12.3. Champs de rapport supplémentaires





Ces informations facultatives sont définies par l'utilisateur et présentées au début du rapport. Elles incluent généralement des informations sur le dossier, l'enquêteur et les détails de l'organisation.

Chaque enregistrement d'informations facultatives contient les informations suivantes :

Nom	Nom du champ de rapport.
Obligatoire	Indique que le champ doit être renseigné pour générer le rapport.
Type	Types d'entrée : **Chaîne** ou **Liste**.
Valeur par défaut	Contenu par défaut.

Vous pouvez ajouter des champs de rapport, et modifier et supprimer des champs, à votre convenance.

12.3.1. Ajouter un champ de rapport

1) Cliquez sur **Ajouter**.

   Une nouvelle ligne est ajoutée au tableau.

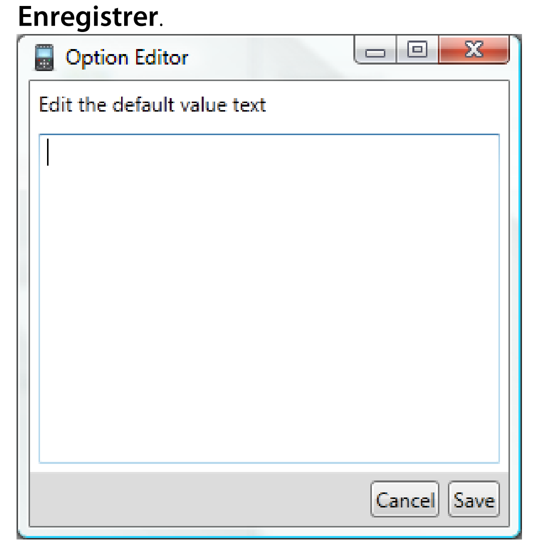
2) Dans la colonne **Nom**, saisissez le nom à afficher.
3) Sélectionnez **Obligatoire** si ce champ doit être rempli pour que l'utilisateur puisse générer le rapport.

4) Dans la liste **Type**, sélectionnez une des options suivantes :

- **Chaîne** pour les champs de saisie de texte ;
- **Liste** pour une liste d'options spécifiées.

5) Dans le champ **Valeur par défaut**, définissez le contenu par défaut :

- Pour le type **Chaîne**, saisissez la chaîne par défaut. Pour une chaîne de plusieurs lignes, cliquez sur , saisissez la chaîne par défaut dans l'Éditeur d'option, puis cliquez sur **Enregistrer**.





- Pour le type **Liste**, cliquez sur , saisissez les éléments de la liste, un par ligne, puis cliquez sur **Enregistrer**.

12.3.2. Supprimer un champ de rapport

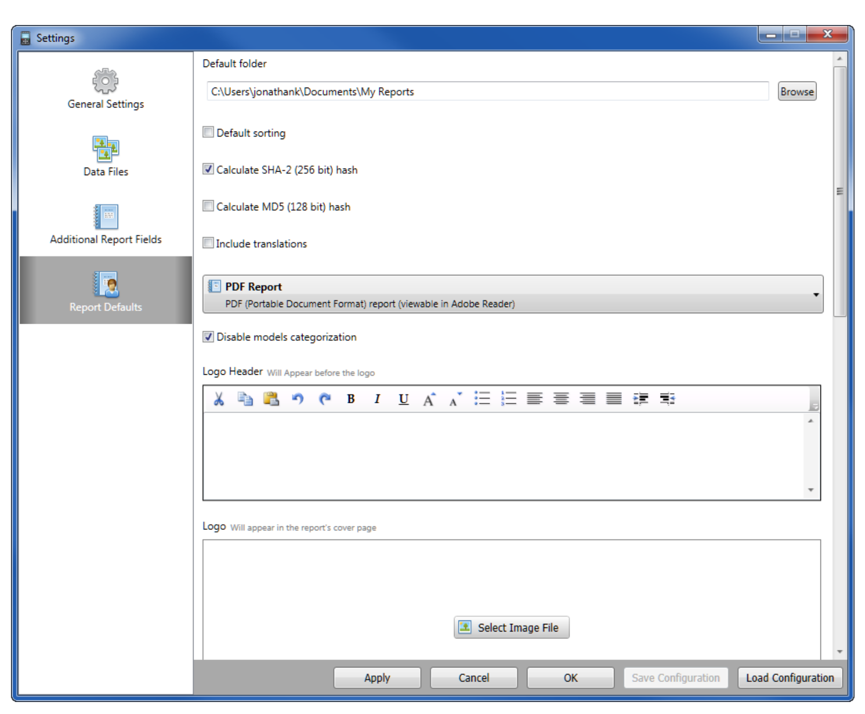
- Pour supprimer un champ de rapport, cliquez sur .

12.3.3. Modifier un champ de rapport

- Pour modifier un champ de rapport, suivez les étapes 2 à 5 de la section ***Ajouter un champ de rapport*** (page ***172***), et modifiez les paramètres à votre convenance.

12.4. Paramètres par défaut du rapport

Les **Paramètres par défaut du rapport** vous permettent de modifier la présentation du rapport.





REMARQUE : Faites défiler vers le bas pour voir tous les champs.

1) Dans la liste **Type de rapport**, sélectionnez le type de rapport que vous souhaitez modifier.
2) Pour les rapports au format Excel, définissez les options suivantes :
   - **Dossier par défaut** – saisissez le chemin du dossier dans lequel vous souhaitez enregistrer les rapports que vous générez pour ce type de rapport.
   - Sélectionnez **Tri par défaut** pour trier les éléments inclus dans le rapport généré en fonction du tri par défaut défini par Cellebrite pour chaque type de fichier analysé et de données, ou désélectionnez **Tri par défaut** pour trier les éléments en fonction du champ de tri sélectionné et de l'ordre de tri (croissant ou décroissant) défini par l'utilisateur dans chaque tableau d'affichage de données.
   - **Calculer le hachage SHA-2 (256 bits)** et **Calculer le hachage MD5 (128 bits)** – sélectionnez les clés de hachage MD5 et SHA256 calculées à ajouter à chaque élément des fichiers de données dans le rapport généré. Désactivez ces options pour raccourcir la durée du processus de création du rapport pour les projets de taille importante.
   - **Inclure les traductions** – sélectionnez cette option pour inclure le texte traduit dans le rapport.
   - **Caractère générique pour les caractères non imprimables** – définissez le caractère générique qui remplace les caractères non imprimables.
   - **Format du fichier de sortie** – définissez le format de sortie du fichier tableur, au choix :
     * **XLSX** – format de fichier Excel actuel.

     * **XLS** – ancien format de fichier Excel.

* **ODS** – format de fichier tableau OpenOffice.

- **Rapport Excel compatible avec OpenOffice** – sélectionnez cette option pour vous assurer que le rapport Excel pourra être ouvert sous OpenOffice.
- **Générer les données d'identification du contact** – sélectionnez cette option pour ajouter une feuille au rapport Excel contenant une liste des contacts uniques en fonction du type.

3) Pour les rapports au format HTML, définissez les options suivantes :

- **Dossier par défaut** – saisissez le chemin du dossier dans lequel vous souhaitez enregistrer les rapports que vous générez pour ce type de rapport.
- Sélectionnez **Tri par défaut** pour trier les éléments inclus dans le rapport généré en fonction du tri par défaut défini par Cellebrite pour chaque type de fichier analysé et de données, ou désélectionnez **Tri par défaut** pour trier les éléments en fonction du champ de tri sélectionné et de l'ordre de tri (croissant ou décroissant) défini par l'utilisateur dans chaque tableau d'affichage de données.
- **Calculer le hachage SHA-2 (256 bits)** et **Calculer le hachage MD5 (128 bits)** – sélectionnez les clés de hachage MD5 et SHA256 calculées à ajouter à chaque élément des fichiers de données dans le rapport généré. Désactivez ces options pour raccourcir la durée du processus de création du rapport pour les projets de taille importante.
- **Inclure les traductions** – sélectionnez cette option pour inclure le texte traduit dans le rapport.
- **Désactiver la catégorisation des modèles** – sélectionnez cette option pour désactiver la séparation et générer un rapport dans lequel chaque élément de données est généré comme une section unique, sans séparation en sous-catégories. Par défaut, le rapport créé



est organisé en catégories, et chaque catégorie du groupe d'éléments de données est générée comme section séparée du rapport. Par exemple, lorsque vous générez un rapport avec des SMS, cochez cette case pour générer les SMS sous forme de liste unique, ou décochez-la pour créer une liste distincte pour chaque catégorie de SMS (reçus, envoyés, brouillons, etc.).

- **En-tête du logo** – saisissez et personnalisez le format du texte qui s'affiche dans l'en-tête du rapport avant le logo.
- **Logo** – cliquez sur **Sélectionner un fichier image** pour ajouter l'image du logo à l'en-tête du rapport. Les formats compatibles sont : BMP, JPG, GIF et PNG.
- **Pied de page du logo** – saisissez et personnalisez le format du texte qui s'affiche dans le pied de page du rapport après le logo.
- **Afficher les totaux pour les éléments exclus du rapport** – ajoute une colonne **Total** au rapport qui affiche le nombre total d'éléments exclus du rapport.
- **Afficher le statut complet des éléments supprimés** – inclut le statut (**Intact**, **Supprimé** ou **Inconnu**) des éléments supprimés dans le rapport généré. Lorsque cette option n'est pas sélectionnée, le statut des éléments supprimés est simplement « Oui », et reste vide pour les autres statuts.
- **Nombre de lignes de l'aperçu d'e-mail** – définit le nombre maximum de lignes affiché dans le rapport pour chaque e-mail.
- **Afficher le corps entier de l'e-mail** – affiche la totalité du corps du message.
- **Nombre de messages par conversation instantanée** – définit le nombre maximum de lignes affiché dans le rapport pour chaque conversation instantanée.

- **Afficher tous les messages des conversations instantanées** – affiche dans le rapport la totalité des messages des conversations instantanées.
- **Diviser le rapport HTML** – chaque section du rapport commence sur une nouvelle page.

4) Pour les rapports au format PDF, définissez les options suivantes :

- **Dossier par défaut** – saisissez le chemin du dossier dans lequel vous souhaitez enregistrer les rapports que vous générez pour ce type de rapport.
- Sélectionnez **Tri par défaut** pour trier les éléments inclus dans le rapport généré en fonction du tri par défaut défini par Cellebrite pour chaque type de fichier analysé et de données, ou désélectionnez **Tri par défaut** pour trier les éléments en fonction du champ de tri sélectionné et de l'ordre de tri (croissant ou décroissant) défini par l'utilisateur dans chaque tableau d'affichage de données.
- **Calculer le hachage SHA-2 (256 bits)** et **Calculer le hachage MD5 (128 bits)** – sélectionnez les clés de hachage MD5 et SHA256 calculées à ajouter à chaque élément des fichiers de données dans le rapport généré. Désactivez ces options pour raccourcir la durée du processus de création du rapport pour les projets de taille importante.
- **Inclure les traductions** – sélectionnez cette option pour inclure le texte traduit dans le rapport.
- **Désactiver la catégorisation des modèles** – sélectionnez cette option pour désactiver la séparation et générer un rapport dans lequel chaque élément de données est généré comme une section unique, sans séparation en sous-catégories. Par défaut, le rapport créé est organisé en catégories, et chaque catégorie du groupe d'éléments de données est générée comme section séparée du rapport. Par exemple, lorsque vous générez un rapport



avec des SMS, cochez cette case pour générer les SMS sous forme de liste unique, ou décochez-la pour créer une liste distincte pour chaque catégorie de SMS (reçus, envoyés, brouillons, etc.).

- **En-tête du logo** – saisissez et personnalisez le format du texte qui s'affiche dans l'en-tête du rapport avant le logo.
- **Logo** – cliquez sur **Sélectionner un fichier image** pour ajouter l'image du logo à l'en-tête du rapport. Les formats compatibles sont : BMP, JPG, GIF et PNG.
- **Pied de page du logo** – saisissez et personnalisez le format du texte qui s'affiche dans le pied de page du rapport après le logo.
- **Afficher les totaux pour les éléments exclus du rapport** – ajoute une colonne **Total** au rapport qui affiche le nombre total d'éléments exclus du rapport.
- **Afficher le statut complet des éléments supprimés** – inclut le statut (**Intact**, **Supprimé** ou **Inconnu**) des éléments supprimés dans le rapport généré. Lorsque cette option n'est pas sélectionnée, le statut des éléments supprimés est simplement « Oui », et reste vide pour les autres statuts.
- **Nombre de lignes de l'aperçu d'e-mail** – définit le nombre maximum de lignes affiché dans le rapport pour chaque e-mail.
- **Afficher le corps entier de l'e-mail** – affiche la totalité du corps du message.
- **Nombre de messages par conversation instantanée** – définit le nombre maximum de lignes affiché dans le rapport pour chaque conversation instantanée.
- **Afficher tous les messages des conversations instantanées** – affiche dans le rapport la totalité des messages des conversations instantanées.

5) Pour les rapports au format package UFED, définissez les options suivantes :

- **Dossier par défaut** – saisissez le chemin du dossier dans lequel vous souhaitez enregistrer les rapports que vous générez pour ce type de rapport.
- Sélectionnez **Tri par défaut** pour trier les éléments inclus dans le rapport généré en fonction du tri par défaut défini par Cellebrite pour chaque type de fichier analysé et de données, ou désélectionnez **Tri par défaut** pour trier les éléments en fonction du champ de tri sélectionné et de l'ordre de tri (croissant ou décroissant) défini par l'utilisateur dans chaque tableau d'affichage de données.
- **Calculer le hachage SHA-2 (256 bits)** et **Calculer le hachage MD5 (128 bits)** – sélectionnez les clés de hachage MD5 et SHA256 calculées à ajouter à chaque élément des fichiers de données dans le rapport généré. Désactivez ces options pour raccourcir la durée du processus de création du rapport pour les projets de taille importante.

6) Pour les rapports au format Word, définissez les options suivantes :

- **Dossier par défaut** – saisissez le chemin du dossier dans lequel vous souhaitez enregistrer les rapports que vous générez pour ce type de rapport.
- Sélectionnez **Tri par défaut** pour trier les éléments inclus dans le rapport généré en fonction du tri par défaut défini par Cellebrite pour chaque type de fichier analysé et de données, ou désélectionnez **Tri par défaut** pour trier les éléments en fonction du champ de tri sélectionné et de l'ordre de tri (croissant ou décroissant) défini par l'utilisateur dans chaque tableau d'affichage de données.
- **Calculer le hachage SHA-2 (256 bits)** et **Calculer le hachage MD5 (128 bits)** – sélectionnez les clés de hachage MD5 et SHA256 calculées à ajouter à chaque élément des



fichiers de données dans le rapport généré. Désactivez ces options pour raccourcir la durée du processus de création du rapport pour les projets de taille importante.

- **Inclure les traductions** – sélectionnez cette option pour inclure le texte traduit dans le rapport.
- **Désactiver la catégorisation des modèles** – sélectionnez cette option pour désactiver la séparation et générer un rapport dans lequel chaque élément de données est généré comme une section unique, sans séparation en sous-catégories. Par défaut, le rapport créé est organisé en catégories, et chaque catégorie du groupe d'éléments de données est générée comme section séparée du rapport. Par exemple, lorsque vous générez un rapport avec des SMS, cochez cette case pour générer les SMS sous forme de liste unique, ou décochez-la pour créer une liste distincte pour chaque catégorie de SMS (reçus, envoyés, brouillons, etc.).
- **En-tête du logo** – saisissez et personnalisez le format du texte qui s'affiche dans l'en-tête du rapport avant le logo.
- **Logo** – cliquez sur **Sélectionner un fichier image** pour ajouter l'image du logo à l'en-tête du rapport. Les formats compatibles sont : BMP, JPG, GIF et PNG.
- **Pied de page du logo** – saisissez et personnalisez le format du texte qui s'affiche dans le pied de page du rapport après le logo.
- **Afficher les totaux pour les éléments exclus du rapport** – ajoute une colonne **Total** au rapport qui affiche le nombre total d'éléments exclus du rapport.
- **Afficher le statut complet des éléments supprimés** – inclut le statut (**Intact**, **Supprimé** ou **Inconnu**) des éléments supprimés dans le rapport généré. Lorsque cette option n'est pas

sélectionnée, le statut des éléments supprimés est simplement « Oui », et reste vide pour les autres statuts.

- **Nombre de lignes de l'aperçu d'e-mail** – définit le nombre maximum de lignes affiché dans le rapport pour chaque e-mail. Le rapport inclut des liens vers les fichiers texte contenant la totalité des e-mails.
- **Afficher le corps entier de l'e-mail** – sélectionnez cette option pour afficher la totalité du corps du message.
- **Nombre de messages par conversation instantanée** – définit le nombre maximum de lignes affiché dans le rapport pour chaque conversation instantanée.
- **Afficher tous les messages des conversations instantanées** – affiche dans le rapport la totalité des messages des conversations instantanées.

7) Pour les rapports au format XML, définissez les options suivantes :

- **Dossier par défaut** – saisissez le chemin du dossier dans lequel vous souhaitez enregistrer les rapports que vous générez pour ce type de rapport.
- Sélectionnez **Tri par défaut** pour trier les éléments inclus dans le rapport généré en fonction du tri par défaut défini par Cellebrite pour chaque type de fichier analysé et de données, ou désélectionnez **Tri par défaut** pour trier les éléments en fonction du champ de tri sélectionné et de l'ordre de tri (croissant ou décroissant) défini par l'utilisateur dans chaque tableau d'affichage de données.
- **Calculer le hachage SHA-2 (256 bits)** et **Calculer le hachage MD5 (128 bits)** – sélectionnez les clés de hachage MD5 et SHA256 calculées à ajouter à chaque élément des



fichiers de données dans le rapport généré. Désactivez ces options pour raccourcir la durée du processus de création du rapport pour les projets de taille importante.

- **Inclure les traductions :** Sélectionnez cette option pour inclure le texte traduit dans le rapport.

12.5. Enregistrer les paramètres

Enregistrez vos paramètres pour les réutiliser ultérieurement, ou pour les partager avec un autre utilisateur.

1) Dans la fenêtre Paramètres, cliquez sur **Enregistrer la configuration**.
2) Dans la fenêtre Enregistrer sous, accédez à l'emplacement où vous souhaitez enregistrer votre configuration de paramètres, puis cliquez sur **Enregistrer**.

   Les paramètres sont enregistrés dans un fichier de configuration des paramètres UFED Logical Analyzer (*.cnf).

12.6. Charger des paramètres

Chargez votre configuration de paramètres enregistrée.

1) Dans la fenêtre Paramètres, cliquez sur **Charger la configuration**.

2) Dans la fenêtre Ouvrir, accédez l'enregistrement de votre configuration de paramètres, sélectionnez-la (*.cnf), puis cliquez sur **Ouvrir**.

   Les paramètres sont appliqués dans la fenêtre Paramètres.

12.7. Définir les paramètres du projet

Définissez un fuseau horaire unifié et des informations de dossier pour chaque projet.

12.7.1. Définir un fuseau horaire unifié pour le projet

Au cours de l'extraction, un horodateur est extrait par événement.

Pour les événements sortants, l'horodateur est généralement issu de l'une des sources suivantes :

- Heure de l'appareil définie par l'utilisateur (lorsque l'heure de l'appareil a été définie manuellement par l'utilisateur) : les horodateurs sont affichés sans l'heure locale exacte (UTC).
- Heure de l'appareil définie par le réseau (lorsque l'heure de l'appareil est définie automatiquement par le réseau) : les horodateurs sont affichés avec l'heure locale exacte (UTC).

Pour les événements entrants, l'horodateur est généralement issu de l'heure définie par le réseau (l'horodateur affecté par le réseau). Les horodateurs sont affichés avec l'heure locale exacte (UTC).



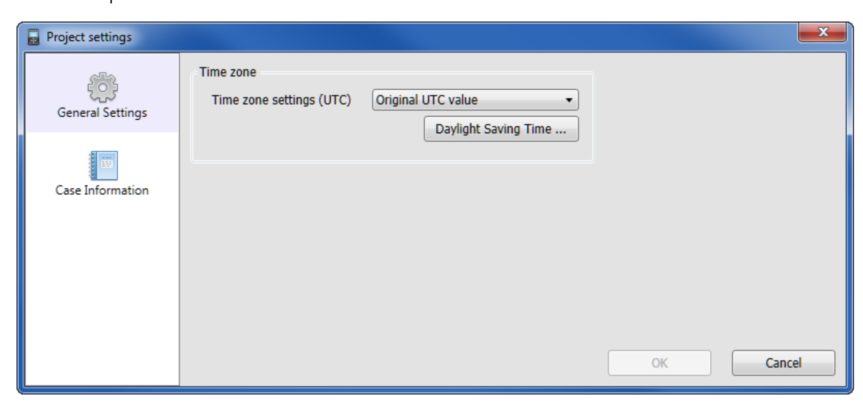
Les horodateurs définis par le réseau dépendent du fuseau horaire dans lequel l'événement s'est produit.

Appliquez un fuseau horaire unifié au projet pour recalculer tous les horodateurs définis par le réseau en fonction du fuseau horaire sélectionné, afin de réunir les événements et de les afficher dans l'ordre dans UFED Logical Analyzer.

Pour appliquer un fuseau horaire unifié au projet :

1) Utilisez une des méthodes suivantes :

- Dans l'onglet **Résumé d'extraction** du projet, cliquez sur **Paramètres du projet**.
- Cliquez sur .



2) Dans la liste **Paramètres de fuseau horaire (UTC)**, sélectionnez :
   - **Valeur UTC originale** pour afficher les horodateurs tels qu'ils ont été enregistrés (sans unification).
   - Un des fuseaux horaires (**UTC -12:00** à **UTC +13:00**) pour recalculer les horodateurs définis par le réseau en fonction du décalage du fuseau horaire.

REMARQUE : Les horodateurs définis par l'utilisateur ne sont pas inclus dans ces nouveaux calculs, et sont affichés tels qu'ils ont été enregistrés.



3) Pour modifier les dates de début et de fin de l'heure d'été, cliquez sur **Heure d'été**.

Daylight Savings

(UTC+00:00) London

	Start		End	
2018	March, 25, 2018	01:00	October, 28, 2018	01:00
2017	March, 26, 2017	01:00	October, 29, 2017	01:00
2016	March, 27, 2016	01:00	October, 30, 2016	01:00
2015	March, 29, 2015	01:00	October, 25, 2015	01:00
2014	March, 30, 2014	01:00	October, 26, 2014	01:00
2013	March, 31, 2013	01:00	October, 27, 2013	01:00
2012	March, 25, 2012	01:00	October, 28, 2012	01:00
2011	March, 27, 2011	01:00	October, 30, 2011	01:00
2010	March, 28, 2010	01:00	October, 31, 2010	01:00
2009	March, 29, 2009	01:00	October, 25, 2009	01:00
2008	March, 30, 2008	01:00	October, 26, 2008	01:00

Back to last saved data | Back to original data | Save | Cancel

a) Pour l'année que vous souhaitez modifier, utilisez le calendrier pour sélectionner les dates de début et de fin, ou modifiez les dates directement. Vous pouvez utiliser le bouton pour supprimer certaines années.

b) Cliquez sur **Revenir aux dernières données enregistrées** pour réinitialiser le tableau à la dernière sauvegarde des données, cliquez sur **Revenir aux données d'origine** pour rétablir les paramètres par défaut du tableau, ou cliquez sur **Enregistrer** pour enregistrer les modifications apportées au tableau.

4) Cliquez sur **OK**.

Le projet est recalculé en fonction du fuseau horaire unifié sélectionné, et le nouveau fuseau horaire est appliqué aux horodateurs définis par le réseau. Les horodateurs des événements affichés dans les fenêtres UFED Logical Analyzer et dans tous les rapports créés ensuite reflètent le fuseau horaire unifié sélectionné.

12.7.2. Définir les informations du dossier

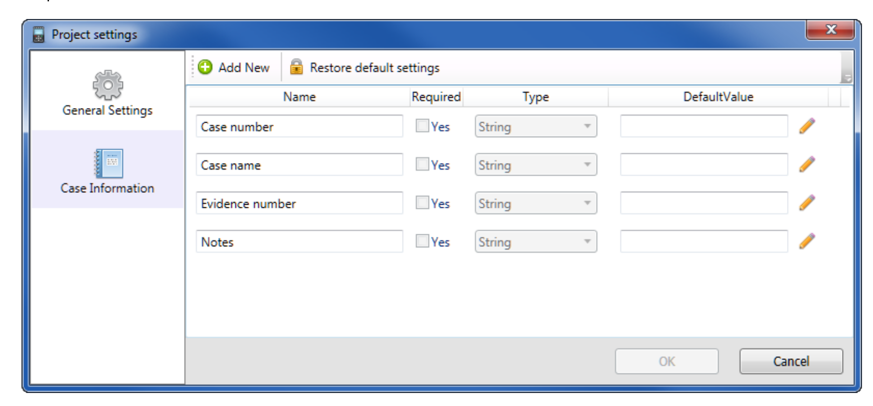
Les paramètres d'informations du dossier sont enregistrés avec le projet. Le numéro de dossier apparaît avec les informations d'extraction sur l'onglet Accueil.

1) Utilisez une des méthodes suivantes :

- Dans l'onglet **Résumé d'extraction** du projet, cliquez sur **Paramètres du projet**.
- Cliquez sur .



2) Cliquez sur **Informations du dossier**.



3) Cliquez sur **Ajouter**.

Certains champs d'informations du dossier sont remplis par défaut.

4) Définissez les paramètres des champs d'information par défauts :

   a) Dans la colonne **Nom**, saisissez les informations correspondantes (par exemple le numéro de dossier, le nom ou des remarques).

   b) Sélectionnez **Obligatoire** si ce champ doit être rempli.

   c) Dans la liste **Type**, sélectionnez une des options suivantes :

      - **Chaîne** pour les champs de saisie de texte ;

- **Liste** pour une liste d'options spécifiées.

d) Dans le champ **Valeur par défaut**, définissez le contenu par défaut :

- Pour le type **Chaîne**, saisissez la chaîne par défaut. Pour une chaîne de plusieurs lignes, cliquez sur , saisissez la chaîne par défaut dans l'Éditeur d'option, puis cliquez sur **OK**.
- Pour le type **Liste**, cliquez sur , saisissez les éléments de la liste, un par ligne, puis cliquez sur **OK**.

5) Pour ajouter des champs d'information supplémentaires, cliquez sur **Ajouter**, puis répétez l'étape 3.
6) Pour supprimer les saisies personnalisées, cliquez sur .
7) Pour rétablir les paramètres par défaut, cliquez sur **Rétablir les paramètres par défaut**.


cellebrite
delivering mobile expertise

Chapitre 13 : **Références**

13.1. Menu Fichier

Ouvrir	Ouvre un fichier pour l'analyser avec le processus d'analyse standard.
Récent	Affiche une liste des projets récents.
Fermer	Ferme le projet actif.
Enregistrer votre session de projet	Enregistre les informations du projet actif générées par l'utilisateur dans un fichier de session UFED Logical Analyzer (*.pas). Consultez la section Enregistrer une session de projet.
Charger une session de projet	Charge un fichier de session UFED Logical Analyzer (*.pas) dans un projet ouvert dans l'arborescence de projet.
Fermer	Ferme UFED Logical Analyzer et toutes les sessions actives.



13.2. Menu Vue

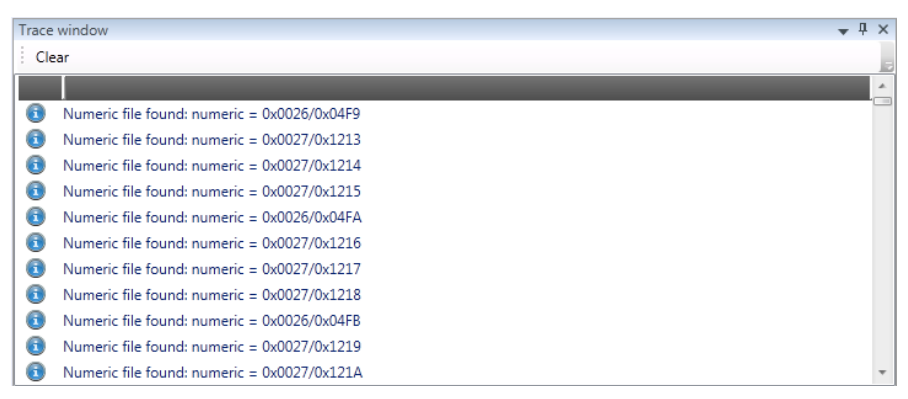
Afficher l'écran d'accueil	Affiche l'onglet **Accueil**. Consultez la section ***Onglet Accueil*** (page ***58***).
Fenêtre Trace	Affiche/Masque la fenêtre Trace en bas de la zone d'affichage des données.

13.2.1. Afficher la fenêtre Trace

Affiche la fenêtre Trace en bas de la zone d'affichage des données, pour voir un journal des actions exécutées au cours de votre session par vous ou UFED Logical Analyzer, par exemple l'activation d'un plug-in.

1) Dans le menu **Vue**, sélectionnez **Fenêtre Trace**.

La fenêtre Trace s'affiche sous la zone d'affichage des données.



2) Pour effacer le journal dans la fenêtre Trace, cliquez sur **Effacer**.
3) Pour fermer la fenêtre Trace, cliquez sur ✕.

La fenêtre Trace peut être masquée ou affichée.

- Pour maintenir ouverte la fenêtre Trace, cliquez sur .
- Pour ne plus maintenir ouverte la fenêtre Trace, cliquez sur .
- Pour afficher la fenêtre Trace lorsqu'elle est masquée, sélectionnez-la ou passez avec le curseur de la souris sur l'onglet.



13.3. Menu Outils

Lire des données depuis UFED	Permet d'extraire des données directement sur l'ordinateur.
Éditeur de liste de surveillance	Ouvre la fenêtre Éditeur de liste de surveillance, qui permet de créer, gérer et exécuter vos listes de surveillance. Consultez la section ***Travailler avec les listes de surveillance*** (page ***86***).
Scanner anti-malware	Ouvre le sous-menu Scanner anti-malware, qui permet d'exécuter la détection de malware sur votre extraction, et de mettre à jour la base de données de signature.
Traduction	Télécharge le package de traduction depuis Internet, installe ce package depuis un fichier ou affiche les langues prises en charge. Consultez la section ***Traduction de données décodées*** (page ***103***).
TomTom	Ouvre le sous-menu TomTom, qui permet d'exporter le fichier d'extraction TomTom et d'importer le fichier XML qui vous est renvoyé.
Paramètres	Accède à la fenêtre Paramètres de l'application. Consultez la section ***Paramètres*** (page ***161***).
Paramètres du projet	Définissez un fuseau horaire unifié et des informations de dossier pour chaque projet. Consultez la section ***Définir les paramètres du projet*** (page ***185***).

13.4. Menu Extraction

Extraction d'appareil iOS	Lance l'extraction d'appareil iOS pour effectuer des extractions d'appareils iOS. Consultez la section ***Effectuer une extraction numérique avancée*** (page ***145***).
Extraire GPS/Appareil de stockage de masse	Lit et enregistre les données d'appareils GPS et de stockage de masse connectés au poste de travail par un câble USB.

13.5. Menu Rapport

Générer un rapport	Génère un résumé du rapport contenant toutes les informations trouvées lors du processus d'analyse. Consultez la section Générer un rapport.



13.6. Menu Aide

Applications prises en charge	Répertorie les applications prises en charge et les versions vérifiées pour les appareils Android et iOS.
Manuel	Ouvre le manuel de l'utilisateur au format PDF.
Activer les cartes Bing en ligne	Active les cartes Bing pour vous permettre d'afficher les emplacements sur une carte. Un accès à Internet et une licence UFED Logical Analyzer valide sont nécessaires.
Lancer la démonstration UFED Link Analysis	Lance l'application UFED Link Analysis.
Afficher les détails de licence	Affiche les informations de licence logicielle ou matérielle (dongle), et vous permet : D'activer ou de charger une nouvelle licence (logicielle ou dongle) ; D'afficher des informations sur les précédents dongles qui ont été connectés à ce poste de travail ; De désactiver une licence logicielle ; De contacter l'assistance et le service des ventes Cellebrite par e-mail.
Zipper les fichiers journaux	Zippe les fichiers journaux et ouvre le dossier dans lequel les fichiers zippés sont enregistrés.

Zipper les fichiers journaux avec informations système	Zippe les fichiers journaux et inclut des informations détaillées concernant le système d'exploitation, les pilotes, les données d'application, les journaux d'événements, etc. Ces informations peuvent être utilisées pour analyser les cas de rapport.
À propos de UFED Physical Analyzer	Fournit des informations sur la version installée de UFED Logical Analyzer.


cellebrite
delivering mobile expertise

A

C

D

E


cellebrite
delivering mobile expertise


cellebrite
delivering mobile expertise

V

Z